Выдержка из *International Review of the Red Cross,* том 99, № 904,
тема номера «Migration and displacement»

МЕЖДУНАРОДНЫЙ
ЖУРНАЛ
Красного Креста

Миграция и защита данных: как не причинить вреда в век массовых вынужденных перемещений, тотальной слежки и «больших данных»

Бен Хейз

Бен Хейз — британский исследователь и консультант по вопросам прав человека, защиты данных и прикладной этики в таких сферах, как противодействие терроризму, международная безопасность, пограничный контроль, поддержание правопорядка, гуманитарная деятельность и НИОКР. Занимается оценкой эффективности мероприятий по защите данных, разработал нормативные документы о защите данных для МККК, Международной Федерации обществ Красного Креста и Красного Полумесяца, Управления Верховного комиссара ООН по делам беженцев (УВКБ), Европейской комиссии, других учреждений и частных компаний. Является научным сотрудником Транснационального института, сотрудником Научно-исследовательского института по вопросам мира (Осло) и фонда «Коллектив безопасности человека», директором компании Data Protection Support & Management Ltd.

Краткое содержание

В данной статье рассмотрены ключевые проблемы в области защиты данных, с которыми сталкиваются гуманитарные организации, оказывающие помощь беженцам, лицам, перемещенным внутри страны,

и мигрантам. Этим проблемам придается особое значение по нескольким причинам: гуманитарный сектор столкнулся с вопросами защиты данных относительно недавно; гуманитарным организациям необходимо быстро внедрять инновации; глобальные коммуникационные сети, которые используются при внедрении многих подобных инноваций, по определению не защищены от слежки со стороны государств; государства задействуют все более изощренные меры принуждения, чтобы предотвратить незаконные виды миграции, и (или) следят за гуманитарными организациями и подрывают их работу. В первой части статьи кратко описаны проблемы соблюдения основных прав, порождаемые современным подходом к управлению миграцией, который основан на сборе различных данных. Во второй части изложены опасения, вызванные «гуманитаризмом, которым движут данные», и «массовой слежкой», и показано, как гуманитарные организации могут невольно усугубить эти проблемы. В третьей части оцениваются конкретные трудности при защите данных, с которыми сталкиваются гуманитарные организации, нормы и подходы, разработанные ими для преодоления этих трудностей. Статья завершается кратким обзором технических и политических изменений, влияющих на соблюдение гуманитарными организациями своих правовых и этических обязательств, и призывом ко всему сектору наладить сотрудничество, чтобы расширить сферу действия норм защиты данных и юридического запрещения кибератак со стороны государственных субъектов.

Ключевые слова: миграция, пограничный контроль, иммиграция, убежище, беженцы, слежка, проверка на благонадежность, большие данные, гуманитарная деятельность, защита данных, конфиденциальность, права человека.

: : : : : : :

Вы добрались до лагеря беженцев, вас мучает голод, вы в отчаянии. Чтобы получить продукты питания и предметы первой необходимости, вы должны добровольно сдать биометрические данные, то есть согласиться отсканировать радужную оболочку глаза и сдать отпечатки пальцев. Проходит несколько лет, вы живете в стране, которая приняла новый закон о распространении ее юрисдикции на данные в облачном хранилище той организации, которая вам помогла. Получив ваши отпечатки пальцев, спецслужбы теперь могут выяснить не только ваше этническое происхождение, иммиграционный статус, потребительские предпочтения и финансовое положение, но и узнать о ваших передвижениях. В некоторых случаях органы власти могут оказывать на вас давление, продолжая собирать данные о вас. Тот факт, что к «гуманитарным данным» открыт доступ и они могут использоваться в иных, а не в гуманитарных целях, например для борьбы с терроризмом или управления миграционными потоками (что понятно

и важно с определенной точки зрения), подвергает людей серьезным, хотя и потенциально правомерным рискам (это, например, арест, отказ на въезд в страну и т. д.)[1].

Введение

В данной статье рассмотрены ключевые проблемы в области защиты данных, с которыми сталкиваются гуманитарные организации (ГО), оказывающие помощь беженцам, лицам, перемещенным внутри страны, и мигрантам. Важность этих проблем обусловлена многими причинами, но четыре из них особенно актуальны для нашего обсуждения. Первая заключается в том простом факте, что гуманитарный сектор озаботился вопросами защиты данных относительно недавно. Нельзя сказать, что до сих пор ГО несерьезно относились к этим вопросам, например не просили согласия получателей помощи, не убеждались в достоверности полученных данных, не соблюдали нормы конфиденциальности. Понятно, что такие практические подходы уже давно стали неотъемлемой частью их повседневной работы. Однако в целом сектор лишь недавно начал внедрять международные нормы защиты данных и соблюдать их. Поборники конфиденциальности справедливо указывали на то, что ГО отстают от развития требований законов о защите конфиденциальности и личных данных[2], и это побудило некоторые ГО срочно устранять указанные недостатки. Однако традиционно гуманитарная деятельность находилась на периферии внимания, когда речь шла о защите данных (с точки зрения как правовых норм, так и числа сторонников перемен), по крайней мере, в сравнении с другими секторами[3].

Такое отсутствие внимания критично, поскольку особенности чрезвычайных ситуаций или конфликтов, когда гуманитарные организации обыкновенно и оказывают помощь, порождают неимоверные трудности при реализации ключевых принципов защиты данных. На территориях, где ведется гуманитарная деятельность, зачастую власть либо отсутствует, либо оставляет желать лучшего, и может показаться, что защита данных там — последняя задача в списке приоритетов, но нельзя рассматривать эти проблемы в отрыве от более широкого общественного, политического или правового контекста. Напротив, в нынешнем мире при всем масштабе

1 Anja Kaspersen and Charlotte Lindsey-Curtet, "The Digital Transformation of the Humanitarian Sector", *Humanitarian Law & Policy Blog*, 5 December 2016, доступно по адресу: blogs.icrc.org/law-and-policy/2016/12/05/digital-transformation-humanitarian-sector/ (все интернет-ресурсы проверены в августе 2017 г.).

2 Anna Crowe, "A Paucity of Privacy: Humanitarian, Development Organizations Need Beneficiary Data Protection Policies", *Privacy International*, 28 November 2013, доступно по адресу: https://privacyinternational.org/blog/1414/paucity-privacy-humanitarian-development-organisations-need-beneficiary-data-protection.

3 Резолюция 1990 г. Генеральной Ассамблеи ООН «Руководящие принципы регламентации компьютеризированных карточек, содержащих данные личного характера» является самым значительным исключением, но она была принята лишь на начальном этапе внедрения принципов защиты данных в компьютерные системы ООН и не относится к гуманитарной деятельности как таковой (см.: резолюция ГА ООН № 45/95 от 14 декабря 1990 г.).

гуманитарной помощи мигрантам и беженцам постоянно звучат и все более настойчивые требования ограничить миграцию и усилить охрану границ. На практике эти требования уже вылились во все более изощренные основанные на данных методы «управления миграцией», а они, в свою очередь, породили новые проблемы в сфере соблюдения прав человека и защиты данных. И это вторая архиважная проблема, которой посвящена данная статья.

С последствиями этих перемен ГО должны бороться в первую очередь как защитники прав и интересов собственных получателей помощи, но и потому, что они сами все более активно применяют те же («функционально совместимые») технологии и работают в партнерстве с органами власти, которых по разным причинам также интересуют подобные данные. Тем же ГО, которые внедряют инновации и используют новые возможности «гуманитарной деятельности, которой движут данные»[4], придется положиться на глобальную инфраструктуру телекоммуникаций, а она не защищена от слежки и в нее могут внедриться государственные и негосударственные субъекты. ГО могут стать мишенью как дружественных, так и враждебных разведслужб, поэтому третья ключевая проблема, рассмотренная ниже, это риск для ГО превратиться в «пособников слежки».

Третья проблема связана с четвертой, а именно, как говорил К. Маркс[5], с «двойственным характером», присущим системам, которые в XXI веке определяют как международные передвижения, так и доставку гуманитарной помощи. Здесь технологии больших данных обещают все — от надежных границ и прогноза преступлений до эффективного распределения гуманитарной помощи. Уже сейчас доступ на территории и оказание гуманитарной помощи все больше регулируются нормами, основанными на слежке и социальной сортировке, практикой включения в общество одних людей и исключения из него других, управления общественной жизнью.

Все это приводит к ощутимым последствиям для ГО, соблюдающих принцип «не навреди», так как сказывается на их деятельности и репутации, на основных правах и безопасности получателей помощи. В развитых странах взлом данных может причинить их жертвам неудобства или привести к финансовым потерям, но для беженцев и их родственников, оставшихся дома, он может стать смертельной угрозой[6]. Мероприятия по защите данных могут показаться слабым противовесом «массовой слежке», о которой рассказал Эдвард Сноуден[7], или же «чрезвычайным мерам по проверке

4 См., например: Patrick Meier, "New Information Technologies and Their Impact on the Humanitarian Sector", *International Review of the Red Cross*, Vol. 93, No. 884, 2011.

5 Эта аналогия, в свою очередь, позаимствована из работы Томаса Матиенсена «Глобализация контроля: становление интегрированной системы слежки в Европе» (Thomas Mathiesen, *On Globalisation of Control: Towards an Integrated Surveillance System in Europe*, Statewatch, London, November 1999, p. 1.).

6 A. Kaspersen and C. Lindsey-Curtet (примечание 1 выше).

7 Эдвард Сноуден — разоблачитель, передавший журналистам газет «Guardian» и «Washington Post» множество документов о работе разведывательных служб. В них содержались оперативные подробности о глобальных системах слежки США и их партнеров в Австралии, Великобритании и Канаде; обе газеты получили Пулитцеровскую премию за свои публикации на эту тему.

мигрантов», которые требует ввести президент США Дональд Трамп[8]. Однако соблюдение строгих требований защиты данных — один из немногих доступных вариантов для тех ГО, которые стремятся ответственно внедрять инновации, защищать свою репутацию от последствий утери данных или кибератак, а также решить те внушительные проблемы, возникающие в связи с большими данными и правительственными методами принуждения[9].

Данная статья разделена на три основные части. В первой части развиваются идеи, изложенные в данном введении; кратко описаны нынешние ключевые черты механизмов управления международной миграцией и порожденные ими угрозы для соблюдения основных прав. Во второй части кратко изложены опасения, вызванные «гуманитарной деятельностью, которой движут данные», на примере документов, получивших огласку благодаря Эдварду Сноудену, и показано, как ГО могут невольно усугубить эти проблемы, превращаясь в «пособников слежки». И наконец, учитывая чрезмерно упрощенный и смахивающий на погоню за сенсациями критический подход к инновациям в гуманитарной деятельности, в третьей части предпринята попытка более детально и при необходимости с технической точки зрения оценить те уникальные проблемы защиты данных, с которыми сталкиваются ГО в работе с мигрантами и беженцами. Там же приведены некоторые нормы и практические подходы, которые они разработали для решения этих проблем. Статья завершается кратким обзором тех технических и политических изменений, которые определяют работу ГО при соблюдении взятых на себя юридических и этических обязательств, и аргументами о необходимости совместной работы ГО для внедрения в сектор норм защиты данных и запрета кибератак со стороны государственных субъектов.

Секьюритизация международной миграции

В теории международных отношений, в аналитических исследованиях вопросов безопасности и других социологических дисциплинах под «секьюритизацией» понимается процесс превращения некоего явления в «угрозу безопасности»[10]. В результате такой политизации доселе чрезмерные и недо-

8 Sabrina Siddiqui, "Trump Signs 'Extreme Vetting' Executive Order for People Entering the US", *The Guardian*, 27 January 2017, доступно по адресу: www.theguardian.com/us-news/2017/jan/27/donald-trump-muslim-refugee-ban-executive-action.

9 О проблемах, порожденных большими данными, см.: Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Harvard University Press, Cambridge, MA, 2015; Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Penguin, London, 2016; Gry Hasselbalch and Pernille Tranberg, *Data Ethics — The New Competitive Advantage*, Publishare, Copenhagen, 2016. О проблемах, порожденных массовой слежкой и методами принуждения со стороны правительств, см.: Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton, New York, 2015.

10 О происхождении этого вида теории «секьюритизации» см.: Barry Buzan, Ole Wæver and Jaap de Wilde, *Security: A New Framework for Analysis*, Lynne Rienner, Boulder, CO, 1998.

пустимые меры политиков превращаются в приемлемые и нормальные, что было бы невозможно без риторики об угрозах безопасности, реальных или надуманных. Хотя многие спорят о достоинствах и пользе теории «секьюритизации»[11], трудно вообразить более «секьюритизированные» вопросы публичной политики, чем проблемы международной миграции, предоставления убежища и пограничного контроля. В самом деле, даже самые бывалые путешественники с трудом вспомнят недавние, по сути, времена, когда иммиграционные формальности носили в основном процедурный характер, а сканеры персонального досмотра, которыми сегодня утыканы пропускные пункты аэропортов, все еще были уделом научной фантастики.

Миграция издревле была способом выживания, но легальная миграция всегда подразумевает привилегии, ее направляют доминирующая идеология и структуры власти, а визовый режим и правила въезда в страну неотделимы от колониализма, расизма и фашизма[12]. Сегодня как никогда ранее в политической риторике и практических подходах к защите «национальной безопасности» «мигранты», «беженцы» и «нелегалы» представляются в целом как некие объекты. Очевидно, что краткий обзор, приведенный ниже, никоим образом не способен восстановить справедливость в этой сложной и сильно политизированной сфере[13], тем не менее в нем описаны ключевые характеристики общей нормативно-правовой базы, построенной вокруг «данных», в которой, однако, ключевые принципы защиты данных либо оттеснены на периферию, либо обходятся стороной. Эти характеристики: слияние задач пограничного контроля и борьбы с терроризмом; новые технологии установления личности; расползание по всему миру мер контроля миграции; привлечение частных подрядчиков и авторитаризм; более строгие процедуры проверки благонадежности; ограничение актуальных механизмов защиты прав человека.

11 См.: Columba Peoples and Nick Vaughan-Williams, *Critical Security Studies: An Introduction*, Routledge, New York, 2010.

12 См.: Liz Fekete, "The Emergence of Xeno-Racism", *Race & Class*, Vol. 43, No. 2, 2001; Steve Cohen, *Standing on the Shoulders of Fascism: From Immigration Control to the Strong State*, Trentham Books, London, 2002; Liz Fekete, *A Suitable Enemy: Racism, Migration and Islamophobia in Europe*, Pluto Press, London, 2009; Marjory Harper and Stephen Constantine, *Migration and Empire*, Oxford University Press, 2010; Lili Eskinazi, "European Immigration: A Colonial Legacy?", *Alternatives International Journal*, 31 October 2011, доступно по адресу: www.alterinter.org/spip.php?article3694.

13 Данная статья не описывает теории слежки или миграционного контроля и не претендует на это. Также нужно подчеркнуть, что слежка может быть как побочным эффектом несметного множества национальных и международных норм, принятых в этой сфере, так и мотивировкой их инициаторов. Таким же образом отсутствие внимания в данной статье к другим факторам, определяющим развитие ситуации в этой сфере, например к закономерностям миграции, политической ситуации в стране, развитию технологий и бюрократическим порывам повысить эффективность пограничного контроля, ни в коей мере не означает, что они не играют важной роли. Наконец меры по управлению миграцией не везде одинаковы; они могут развиваться в одном четком направлении, но это движение можно описать словами «разрозненная постепенность», этот термин появился в эссе политолога Чарлза Э. Лидблома, опубликованном в 1959 г., см.: Charles E. Lindblom, "The Science of 'Muddling Through'", *Public Administration Review*, Vol. 19, No. 2, 1959.

Миграция и терроризм — есть ли связь?

Первая характеристика — слияние задач пограничного контроля и борьбы с терроризмом после терактов в США 11 сентября 2001 г. Хотя статистика уверяет, что угроза «доморощенного» терроризма значительно превосходит угрозу совершения терактов мигрантами[14] или что в США вероятность стать жертвой теракта намного ниже, чем быть застреленным полицейским или подростком[15], сегодня повсюду границы стали считаться первейшей и наиважнейшей линией обороны против терроризма. В 2002 г. тогдашний президент США Джордж Буш говорил: «Нам нужно знать, кто приезжает к нам в страну, зачем, и действительно ли уезжают те, кто заявлял, что собирается ее покинуть»[16]. Эти слова отражают новую идеологию, к которой могли бы свестись, а по сути, неизбежно свелись все споры о мерах пограничного контроля.

И такая риторика ни в коей мере не ограничена территорией США. В числе первых законодательных актов Европейского союза в ответ на теракты 11 сентября 2001 г. стал документ, утвердивший общую позицию по борьбе с терроризмом, где требуется, чтобы страны-члены заранее проверяли всех лиц, которые ищут убежища на предмет связи с террористами[17]. Данная позиция в свою очередь была заимствована из положений резолюции СБ ООН на эту же тему, не имевших обязательной силы[18]. В последующие 15 лет путешественники всех мастей стали сталкиваться со все более изощренными попытками проверки и профилирования для оценки и устранения рисков, которые они предположительно собою представляют. Подобное развитие событий вымостило дорогу «чрезвычайным мерам по проверке мигрантов», введения которых добивается нынешнее правительство США (см. далее).

Идентификация личности

Вторая характеристика вытекает из первой. После событий 11 сентября 2001 г. все многообразие попыток управлять миграцией свелось к внедрению технических средств установления личности на основе биометрических систем идентификации. Их изначальная цель — проверить с помощью уникального биометрического маркера[19], соответствует ли

14 Alex Nowrasteh, *Terrorism and Immigration: A Risk Analysis*, Cato Institute, Policy Analysis No. 798, Washington, DC, 13 September 2016.

15 Gary Younge, "Trump Fears Terrorists, but more Americans are Shot Dead by Toddlers", *The Guardian*, 8 February 2017, доступно по адресу: www.theguardian.com/commentisfree/2017/feb/08/trump-muslim-terrorists-gun-violence-america-deaths.

16 Adam Entous, "Bush to Seek New Powers in Homeland Security Plan", *Reuters*, 15 July 2002.

17 Council Common Position of 27 December 2001 on Combating Terrorism, *Official Journal of the European Communities*, 2001/930/CFSP, 27 December 2001 (OJ 2001 L 344/90), Art. 16.

18 Резолюция Совета Безопасности ООН 1373 от 28 сентября 2001 г., ст. 3(f).

19 В большинстве биометрических систем пограничных и иммиграционных служб используют либо цифровые фотографии, либо отпечатки пальцев, либо сканы радужной оболочки глаза, или же два таких маркера. Биометрический профиль вносится в базу данных населения страны

личность владельца проездного документа личности человека, которому он был выдан. Однако сегодня такие системы уже внедряются в различных учреждениях охраны правопорядка и слежки. В некоторых странах с сильными традициями защиты гражданских свобод, например в Великобритании и США, обязательная сдача отпечатков пальцев остается за (постепенно исчезающей) запретной чертой, но, несмотря на все эти традиции, биометрическое профилирование уже широко применяется по всему миру и быстро превратилось в норму в отношении к «негражданам» и иностранцам[20].

Сегодня во всем мире биометрическое профилирование уже стало неотъемлемой частью работы служб пограничного контроля, но по мере развития подобных систем растет и сфера их применения. С помощью так называемых «умных систем пограничного контроля» можно отслеживать людей на обширных территориях[21]. К базам биометрических данных уже имеют доступ органы национальной безопасности и охраны правопорядка[22]. Кажется, что законопослушные путешественники уже смирились с тем, что биометрическое профилирование стало условием въезда в страну (конечно, не потому, что у них был иной выбор). Однако принудительное использование биометрических систем, например при решении вопросов предоставления убежища и выдворения органами власти стран ЕС, уже породило пугающие случаи: беженцы и мигранты уродуют пальцы, чтобы не пасть жертвой мер иммиграционного контроля[23]. В ответ на это государства начали вводить меры уголовной ответственности для тех, кто не сдает

и (или) записывается в радиочастотный чип идентификации, встроенный в выдаваемый органами власти проездной документ. И тогда личность любого человека можно установить по базе данных или по проездному документу. Единственным биометрическим маркером, требуемым Международной организацией гражданской авиации, которая устанавливает глобальные стандарты авиаперелетов, является цифровая фотография.

20 Решение ЕС о биометрическом профилировании всех тех, кто ищет убежища, и нелегальных мигрантов на самом деле было принято задолго до событий 11 сентября 2001 г., этот законопроект был разработан еще в 1995 г., а окончательно вступил в силу в 2000 г. После событий 11 сентября 2001 г. ЕС принял решение об обязательной сдаче отпечатков пальцев всеми, кто подает заявку на визу, для всех граждан третьих стран, кому не требуется виза ЕС, всех жителей стран ЕС, являющихся гражданами третьих стран, и для всех владельцев паспорта ЕС (Великобритания воздержалась). См.: Kjetil Rommetveit, "Introducing Biometrics in the European Union: Practice and Imagination", in Ana Delgado (ed.), *Technoscience and Citizenship: Ethics and Governance in the Digital Society*, Springer, Cham, 2016.

21 См.: Ben Hayes and Mathias Vermeulen, *Borderline: The EU's New Border Surveillance Initiatives — Assessing the Costs and Fundamental Rights Implications of EUROSUR and the "Smart Borders" Proposals*, research study, Heinrich Böll Foundation, Berlin, 2012.

22 Например, в законы ЕС, регулирующие все основные базы данных иммигрантов и лиц, ищущих убежища (включая и Шенгенскую информационную систему, систему Eurodac, Визовую информационную систему и предложенную систему «умного пограничного контроля»), были со временем внесены поправки, открывшие к ним доступ службам безопасности и разведки. См.: Costica Dumbrava, "European Information Systems in the Area of Justice and Home Affairs: An Overview", *European Parliamentary Research Service*, May 2017, доступно по адресу: www.europarl.europa.eu/RegData/etudes/IDAN/2017/603923/EPRS_IDA(2017)603923_EN.pdf.

23 См., например: Graeme Culliford, "I've Burned off Tips of My Fingers to Get to UK", *The Sun*, 14 June 2014, доступно по адресу: www.thesun.co.uk/archives/news/900339/ive-burned-off-tips-of-my-fingers-to-get-to-uk/.

отпечатки пальцев по требованию миграционных служб[24]. Символизм этого явления поражает, однако в реальности ужесточение мер борьбы с нерегулярной миграцией уже давно идет рука об руку со все более «экстремальными» попытками обойти их.

Глобальное распространение мер контроля иммиграции

Это явление также отражено в переносе мер иммиграционного контроля из стран назначения в страны происхождения или транзитные страны, для чего им предоставляется техническая помощь, заключаются соглашения о миграционном контроле и «помощи в обмен на торговлю». Такие меры принимают различные формы — от так называемых «проверок до пересечения границы» и обязательства принимать обратно выехавших из страны людей до передачи в эти страны нормативных документов и технологий, зачастую при посредничестве межправительственных организаций.

Можно предположить, что усиление мер иммиграционного контроля просто идет рука об руку с прогрессом и отвечает современности, а богатые страны стараются постепенно ограничить и сократить иммиграцию из бедных стран, однако самые богатые государства мира еще и сознательно экспортируют эти меры. У них двоякая мотивация: во-первых, заручиться поддержкой стран происхождения или транзита мигрантов и беженцев и дать им возможность не пускать непрошеных мигрантов без документов на территории богатых стран, а также оперативно выдворять тех, кто все-таки туда попадет (соглашение о беженцах между ЕС и Турцией — ярчайший пример подобной политики[25]). А во-вторых, упростить сбор сведений о въезжающих в страну и собирать разведданные о других людях, представляющих для них интерес. Наиболее активны в этом учреждения ЕС и входящие в него страны, они оказывают техническую помощь целому ряду стран Центральной и Восточной Европы, Северной и Западной Африки, Ближнего Востока, а в разгар «кризиса» беженцев, к которому всегда приводят вооруженные конфликты, и таким далеким странам, как Шри-Ланка[26]. Подобная помощь охватывает всё, начиная с технических систем иммиграционного контроля и рассмотрения прошений о предоставлении убежища, вплоть до возведения объектов пограничного контроля, обучения сотрудников миграционных и пограничных служб, строительства центров временного содержания и информационных кампаний против нелегальной эмиграции. В нарушение положений о свободном перемещении людей, содержащихся во Всеобщей декларации прав человека (ООН), эта помощь

24 См.: EU Fundamental Rights Agency, *Fundamental Rights Implications of the Obligation to Provide Fingerprints for Eurodac*, Vienna, May 2015.

25 Council of the European Union, "EU-Turkey Statement", Press Release No. 144/16, 18 March 2016.

26 См.: Ben Hayes, Steve Wright and April Humble, "From Refugee Protection to Militarised Exclusion: What Future for 'Climate Refugees'?", in Nick Buxton and Ben Hayes (eds), *The Secure and the Dispossessed: How the Military and Corporations Are Shaping a Climate-Changed World*, Pluto Press, London, 2015.

предусматривает строгие принудительные меры предотвращения «незаконного выезда»[27].

США также предоставили значительный объем технической помощи в этой области, включая технические средства и финансовые средства на закупку систем миграционного контроля, таким странам, как Афганистан, Гана, Йемен, Камбоджа, Кения, Мальдивы, Пакистан, Танзания и Эфиопия[28]. Министр правительства одной из стран, осыпанных этими щедротами, объяснил их причину тем, что «американцы хотят иметь рычаги влияния на нас», получив возможность по своему желанию узнавать о месте нахождения граждан других стран[29]. Невзирая на мотивацию, и об этом будет сказано ниже, неразрывная связь между мерами пограничного контроля, установления личности и вопросами национальной безопасности часто порождает, при получении подобной технической помощи, вопросы о соблюдении прав человека, а их редко обсуждают доноры или получатели пожертвований.

Перекладывание ответственности, приватизация и авторитаризм

Помимо едва прикрытых попыток богатых стран переложить ответственность за судьбу беженцев и лиц, ищущих убежища, на плечи стран победнее, современные подходы к управлению иммиграцией характеризуются растущим вовлечением частного сектора в осуществление соответствующих внутригосударственных и международных мер[30]. Страны ЕС, например, уже ввели юридическую ответственность для транспортных компаний, возложив на них обязанность не перевозить пассажиров без документов или без необходимых документов. Начиная с авиакомпаний и вплоть до водителей грузовиков, все они зачастую облагаются за провоз незаконных пассажиров порядочными штрафами, известными как «санкции против перевозчиков»[31]. Скандальная ситуация складывается и для частных судовладельцев, стремящихся спасти мигрантов с терпящих

27 Например, страны ЕС поставили подразделениям ливийской береговой охраны военные суда. См.: Maurizio Albahari, *Crimes of Peace: Mediterranean Migrations at the World's Deadliest Border*, University of Pennsylvania Press, Philadelphia, 2015, p. 88. См. также: Maggie Michael, "Backed by Italy, Libya Enlists Militias to Stop Migrants", *Associated Press*, 29 August 2017, доступно по адресу: www.apnews.com/9e808574a4d04eb38fa8c688d110a23d. Во Всеобщей декларации прав человека утверждается: «Каждый человек имеет право покидать любую страну, включая свою собственную...» (Всеобщая декларация прав человека, 10 декабря 1948 г., ст. 13(2)).

28 См.: Ben Hayes and Roch Tassé, "Control Freaks: 'Homeland Security' and 'Interoperability'", *DifferenTakes: A Publication of the Population and Development Programme at Hampshire College*, No. 45, Spring 2007.

29 Ильяс Хуссейн Ибрагим, бывший мальдивский государственный министр обороны и национальной безопасности, цит. по: Gus Hosein and Carly Nyst, Aiding Surveillance, Privacy International, London, 2013, p. 55, доступно по адресу: https://www.privacyinternational.org/report/841/aiding-surveillance.

30 См.: Thomas Gammeltoft, "The Migration Control Industry", in Rita Abrahamsen and Anna Leander (eds), *Routledge Handbook of Private Security Studies*, Routledge, London, 2016.

31 См.: Sophie Scholten, *The Privatisation of Immigration Control through Carrier Sanctions*, Brill, Leiden, 2015.

бедствие судов. Теперь им можно спасать только людей, которые вот-вот утонут, в иных случаях им также начинают угрожать и преследовать их в уголовном порядке[32].

В общем, по мере роста зависимости государств от крупномасштабных компьютерных систем и технических средств наблюдения частный сектор стал все больше инвестировать в разработку средств иммиграционного и пограничного контроля и в способы осуществления мер в этой области. Наибольшую выгоду в такой ситуации извлекли оборонный и технологический секторы: уже сегодня значительная часть выручки крупнейших оборонных подрядчиков складывается благодаря диверсификации, которой они достигли, занимаясь всем, что связано с «национальной безопасностью»[33]. Помимо огромных контрактов на укрепление границ и поставку полномасштабных систем наблюдения, приватизация мест содержания уголовных преступников привела к повышению роли частного сектора в управлении лагерями временного содержания мигрантов и осуществлении мер по их выдворению[34]. Передача в частные руки пограничного и иммиграционного контроля неизбежно ставит эффективность и прибыль выше других ценностей и интересов, например ответственности и защиты прав человека.

И наконец возложенные на транспортный сектор обязательства медленно, но верно проникают и в другие сферы общественной и частной жизни, и уже все чаще арендодателей, работодателей, банки, университеты, школы и сотрудников служб здравоохранения юридически обязывают применять правоохранительные меры к своим клиентам и проверять их иммиграционный статус, при этом нарушителей опять же ждут серьезные штрафы. Государственные учреждения и частные лица и компании все чаще становятся инструментом в «битве» с нелегальной иммиграцией, что, несмотря на критику[35] подобных тенденций, все же порождает важные последствия для организаций, приверженных принципам недискриминации и защиты прав человека.

32 См.: Maarten den Heijer, "Frontex and the Shifting Approaches to Boat Migration in the European Union: A Legal Analysis", in Ruben Zaiotti (ed.), *Externalizing Migration Management: Europe, North America and the Spread of "Remote Control" Practices*, Routledge, London, 2016. См. также: Irini Papanicolopulu, "The Duty to Rescue at Sea, in Peacetime and in War: A General Overview", *International Review of the Red Cross*, Vol. 98, No. 902, 2016.

33 См.: Mark Akkerman, *Border Wars: The Arms Dealers Profiting from Europe's Refugee Tragedy*, Transnational Institute, Amsterdam, 2016, доступно по адресу: www.tni.org/en/publication/border-wars.

34 См.: Доклады и вебсайт проекта «Содержание под стражей в глобальном масштабе» (Global Detention Project), доступно по адресу: www.globaldetentionproject.org/.

35 Медицинский персонал и преподаватели вузов оказались в числе тех, кто сопротивляется или отказывается участвовать в таких проверках в тех странах, где они юридически обязательны. См., например: Miranda Wilson, "Academics Refuse to Police Immigration", *Institute of Race Relations News*, 13 May 2009, доступно по адресу: www.irr.org.uk/news/academics-refuse-to-police-immigration/.

Чрезвычайные меры проверки

Все четыре вышеуказанные характеристики вызвали к жизни пятую — наиглавнейшую: накопление персональных данных в целях проверки, профилирования и — как результат — разделения пассажиров и мигрантов на категории законных и подозрительных, заслуживающих въезда в страну и не заслуживающих его, имеющих права и лишенных их и т.д. Как уже говорилось, события 11 сентября 2001 г. стали катализатором этой тенденции, когда ужесточились требования сначала к беженцам и лицам, ищущим убежища, затем — к получателям виз, а затем и к тем, кому виза не требуется.

Средства реализации всего этого таковы: переход на биометрические визы, когда заявления на визу рассматриваются и одобряются в день подачи[36]; раскрытие информации о фамилиях пассажиров и данных, внесенных в системы предварительного сбора информации о пассажирах, с помощью которых органы охраны правопорядка и безопасности еще до поездки получают подробную информацию о них[37]; а также электронные системы разрешения на поездку, разработанные для проверки пассажиров перед посадкой на борт транспортного средства, следующего в страну назначения[38]. Подробности процесса проверки в основном окутаны тайной, но известно, что пассажир должен соответствовать критериям въезда в страну, не нарушать до этого нормы иммиграционного законодательства, его также проверяют по базам данных органов национальной безопасности и контртеррористических служб, например по спискам лиц, которым запрещены полеты, по «контрольным спискам», по санкционным и внешнеполитическим спискам[39]. Этими сведениями государства обмениваются постоянно, например в рамках Шенгенского соглашения, объединения «Пять глаз» и других двусторонних и многосторонних соглашений о сотрудничестве в области безопасности[40].

36 Это, например, относится к визовой информационной системе ЕС.

37 Австралия стала первой использовать систему расширенной информации о пассажирах, а по законам ЕС органы безопасности и разведки имеют право доступа к сведениям о пассажирах, содержащихся в базах бронирования билетов европейских авиакомпаний.

38 В США уже используется система выдачи разрешений на въезд, а ЕС также планирует ввести в действие подобную.

39 Подробности о том, как предположительно работают такие системы, см.: UK House of Commons, Committee of Public Accounts, "E-Borders and Successor Programmes", 27th Report of Session 2015–16, London, 2016. См. также: Julien Jeandesboz, Didier Bigo, Ben Hayes and Stephanie Simon, *The Commission's Legislative Proposals on Smart Borders: Their Feasibility and Costs*, PE 462.613, European Parliament, Brussels, 2013.

40 Страны, подписавшие Шенгенское соглашение, направляют в Шенгенскую информационную систему сведения о людях, которым необходимо отказать во въезде, либо за которыми установлена слежка, а через сеть бронирования «Сирена» обмениваются дополнительной информацией. «Пять глаз» (Five Eyes) — созданный после войны союз разведслужб Австралии, Великобритании, Канады, Новой Зеландии и США. В 2009 г. эти страны приняли «Протокол об обмене данными конференции пяти стран», касающийся биометрической информации (не опубликован). Интерпол, или Международная организация уголовной полиции, также организовал обмен сведениями, которые используются в системах пограничного контроля.

Пока европейская «желтая» пресса с трудом смирялась с мыслью, что и владельцы смартфонов могут нуждаться в защите, полагающейся беженцам[41], европейские правительства воспользовались случаем и ввели собственные «чрезвычайные меры проверки», просто скопировав действия американских и израильских пограничников, которые конфискуют подобные устройства[42]. В начале 2017 г. Дания и Норвегия разработали законопроекты о конфискации смартфонов у беженцев в пунктах их регистрации, чтобы использовать собранные в них данные для двойной проверки, а именно представляют ли лица, ищущие убежища, угрозу безопасности и правомерны ли их прошения о предоставлении убежища[43]. Эти законопроекты породили серьезные сомнения, допустимы ли такие процедуры предоставления убежища, и стали случаем беспримерного вторжения в частную жизнь тех, кто ищет убежища.

Конфиденциальность и защита данных исчезают на границе

А как же быть с конфиденциальностью и нормами защиты данных, которые должны обуздать пристрастие государств к безграничной слежке? Коротко говоря, право на конфиденциальность оказалось относительно неэффективным барьером из-за слишком широкого толкования словосочетания «необходимые и соразмерные» ограничения[44]. Во многом это обусловлено дискриминационным подходом отдельных стран, которые считают, что у иностранцев меньше прав на конфиденциальность, чем у собственных

41 См.: James O'Malley, "Surprised that Syrian Refugees Have Smartphones? Sorry to Break this to You, but You're an Idiot", *The Independent*, 7 September 2015, доступно по адресу: www.independent.co.uk/voices/comment/surprised-that-syrian-refugees-have-smartphones-well-sorry-to-break-this-to-you-but-youre-an-idiot-10489719.html.

42 По поводу США см.: Olivia Solon, "US Border Agents are Doing 'Digital Strip Searches'. Here's How to Protect Yourself", *The Guardian*, 31 March 2017, доступно по адресу: www.theguardian.com/us-news/2017/mar/31/us-border-phone-computer-searches-how-to-protect; по поводу Израиля, см.: "Israel Approves Email Checks at the Border", *Times of Israel*, 24 April 2013, доступно по адресу: www.timesofisrael.com/israel-approves-email-checks-at-the-border/.

43 По поводу Дании см. неопубликованное предложение от 10 февраля 2017 г. по внесению поправок в датский Закон об иностранцах, имеется в распоряжении автора. По поводу Норвегии см. предложение (на норвежском языке) от 11 января 2017 г., доступно по адресу: www.regjeringen.no/contentassets/8c99986c9bd444b6a00d56fe8afca077/visitasjon-horingsnotat-januar-2017.pdf.

44 В ст. 8(2) Европейской конвенции о защите прав человека и основных свобод от 4 ноября 1950 г. (вступила в силу 3 сентября 1953 г.) применительно к праву на частную и семейную жизнь говорится: «Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случая, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других лиц». О том, что превращает простую слежку в средствах коммуникации в «необходимую и соразмерную», см.: Necessary and Proportionate Coalition, "Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance", May 2014, доступно по адресу: www.necessaryandproportionate.org/principles. Решения Суда Европейского союза, которые начинают ограничивать широкий круг допустимых исключений, см.: *Tele2* and *Watson*, Joined Cases Nos C-203/15, C-698/15; *Schrems v. DPC Irl*, Case No. C-362/14; и *Digital Rights Ireland* and *Seitlinger*, Joined Cases Nos C-293/12, C-594/12.

граждан[45]. Что касается норм защиты данных, которые регламентируют обработку персональных данных государственными органами и частными компаниями и дают субъектам данных контроль над такими сведениями, а также право требовать компенсации при их ненадлежащем использовании, то здесь отступления от требований безопасности и государственной политики усугубляются еще и ограничениями географического свойства[46]. Уже более сотни стран приняли в том или ином виде законы или нормы о защите данных[47], однако многие из них не соответствуют требованиям комплексной защиты данных и (или) сильно не дотягивают до высочайших стандартов, разработанных в Европе (сначала Советом Европы, а затем и ЕС)[48].

Принципиально важно, что даже при соблюдении этих высоких стандартов, если данные обрабатываются согласно закону или в интересах национальной безопасности, то такие ключевые принципы защиты данных, как согласие на обработку их владельца и предоставление ему права выбора, либо не применяются, либо их невозможно применить. При этом существенно ограничивается право человека распоряжаться собственными персональными данными (например, иметь к ним доступ, исправлять или уничтожать их)[49]. Эти важные исключения лишь подчеркивают общепринятое сегодня представление о том, что персональные данные пассажиров и мигрантов — «законная добыча» служб национальной безопасности. В 2008 г., критикуя разнообразные предложения по укреплению границ ЕС, руководитель службы защиты данных ЕС заявил: они «изначально подразумевают», что «всех приезжающих» нужно «априори считать потенциальными преступниками» и «следить за ними». Но эти слова были мало кем услышаны[50].

45 См.: Marko Milanovic, "Foreign Surveillance and Human Rights, Part 1: Do Foreigners Deserve Privacy?", *EJIL: Talk! Blog of the European Journal of International Law*, 2013, доступно по адресу: www.ejiltalk.org/foreign-surveillance-and-human-rights-part-1-do-foreigners-deserve-privacy/.

46 Хотя защита данных часто рассматривается как следствие охраны права на конфиденциальность в части информации, которая хранится о людях, она все больше признается основным конституционным правом человека. См., например: Charter of Fundamental Rights of the European Union, 2012/C 326/02, 26 October 2012, Art. 8.

47 См.: DLA Piper, "Data Protection Laws of the World", доступно по адресу: www.dlapiperdataprotection.com/.

48 См., например: Совет Европы, Конвенция о защите прав физических лиц в отношении автоматической обработки персональных данных от 28 января 1981 г. (вступила в силу 1 октября 1985 г.); Регламент Европейского парламента о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, и отменяющую директиву 95/46/EC, 2016/679/EU, 27 апреля 2016 г. (далее — ОРЗД).

49 Описание ключевых принципов защиты данных см.: European Union Agency for Fundamental Rights and Council of Europe — European Court of Human Rights, *Handbook on European Data Protection Law,* 2014, доступно по адресу: www.fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf.

50 European Data Protection Supervisor, *Preliminary Comments of the European Data Protection Supervisor*, Brussels, 3 March 2008, p. 5, доступно по адресу: https://edps.europa.eu/sites/edp/files/publication/08-03-03_comments_border_package_en.pdf.

Пособничество слежке?

Как уже говорилось во введении, упомянутые государственные методы принуждения привели к серьезным последствиям для ГО, чья деятельность и инновации, если они не будут следовать строгим требованиям норм защиты данных, рискуют лишь усугубить проблемы в сфере соблюдения основных прав человека, порожденные массовой слежкой и управлением миграцией на основе данных. Эти опасения были изложены в докладе 2013 г. «Пособничество слежке» инициативной группы «Прайваси Интернэшнл» (Privacy International). В нем показано, каким образом «программы развития и оказания гуманитарной помощи создают в развивающихся странах возможности для слежки»[51]. В докладе рассмотрены четыре инновационные области в секторе развития и в гуманитарном секторе: (i) информационные системы, лежащие в основе программ перевода наличных средств; (ii) системы биометрической идентификации и регистрации избирателей; (iii) использование мобильных телефонов и данных, которые они накапливают и создают, мобильными финансовыми приложениями, службами здравоохранения и в кризисных ситуациях; и (iv) пограничные технические средства наблюдения и технические средства безопасности.

На десятках примеров в докладе показано, что хотя базовые технологии в этих областях «стали в последние годы предметом широкого обсуждения в развитых западных демократиях»[52], «все попытки критически осмыслить потенциальные вредные последствия их внедрения в программы развития и гуманитарную деятельность постоянно терпят неудачу, а следовательно, и попытки обсудить юридические и технические меры предосторожности, необходимые для соблюдения прав жителей развивающихся стран»[53]. Заслуженно критиковались и учреждения ООН, доноры, международные неправительственные организации, участники проектов развития и ГО. Также критике подверглись такие основополагающие стратегические документы, как «Гуманитарность в сетевой век»[54] Управления ООН по координации гуманитарных вопросов (УКГВ) и «Новое глобальное партнерство», который подготовила группа экспертов ООН высокого уровня[55] в рамках разработки повестки дня сектора развития на период после 2015 г. Эти документы вызвали упреки за то, что они «уделяют мало внимания потенциальным последствиям для конфиденциальности, которые обусловлены внедрением новых технологий и средств анализа данных»[56]. В заключение доклад предупреждает о рисках установить слишком низкую планку в защите прав человека, если следовать принципу «не нав-

51 G. Hosein and C. Nyst (примечание 29 выше).
52 Ibid., p. 8.
53 Ibid., p. 7.
54 OCHA, *Humanitarianism in the Network Age*, OCHA Policy and Study Series, Geneva, 2013.
55 UN, *A New Global Partnership: Eradicate Poverty and Transform Economies through Sustainable Development: The Report of the High-Level Panel of Eminent Persons on the Post-2015 Development Agenda, 2013*, New York, 2013.
56 G. Hosein and C. Nyst (примечание 29 выше), p. 9.

реди», который так любят работники гуманитарного сектора. Доклад предлагает ставить такую цель: не просто избегать нарушений прав человека при оказании гуманитарной помощи, но активно популяризировать и защищать эти права[57].

Помимо ответственного внедрения инноваций, ГО сталкиваются и с другой проблемой, порожденной всплывшей информацией о слежке. Быстрое развитие сначала мобильной связи, а затем и смартфонов[58] породило огромные возможности не только в сфере связи, но и в деле защиты и помощи мигрантам и беженцам, нуждающимся в поддержке ГО. Однако, как отмечено во введении данной статьи, эти же изменения открыли перед органами власти громадные возможности для слежки, что привело к важным последствиям в восприятии информационно-коммуникационных технологий (ИКТ) и в их использовании в ситуациях, когда люди могут пострадать или стать жертвой злоупотреблений, если их обнаружат. Некоторые ГО еще не осознали их, и кажется, будто они полагают, что люди в нужде с радостью сообщат свои персональные данные любому, кто их попросит, либо что конфиденциальность, по сути, — всего лишь западная концепция, не особо популярная в других культурах или обстоятельствах. Однако организации «Открытый университет» (The Open University) и «Мир СМИ Франции» (France Médias Monde) тщательно изучили, каким образом направляющиеся в Европу мигранты пользуются смартфонами и социальными сетями, и это дало им основания полагать, что такая точка зрения ошибочна[59]. Среди прочего эта работа показала, что «мигранты боятся как традиционной слежки, например со стороны государственных органов, так и слежки со стороны других мигрантов (!) из своего окружения», а в результате «они скрывают в социальных сетях и онлайн свою личность, прячась за аватарками и псевдонимами»[60], что «беженцы не раскрывают онлайн свои персональные данные, предпочитая анонимность из-за страхов расправы, слежки, лишения свободы и (или) депортации»[61] и что они общаются с родными и друзьями «в основном в WhatsApp, убежденные в том,

57 G. Hosein and C. Nyst (примечание 29 выше), pp. 56–58. См. также: Kristin Bergtora Sandvik, Katja Lindskov Jacobsen and Sean Martin McDonald, "Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation", *International Review of Red Cross,* Vol. 99, No. 904, 2017.

58 Согласно исследованиям «Открытого университета» и «Мира СМИ Франции», «мобильными телефонами пользуется 98% жителей Ближнего Востока и Северной Африки, 84% — пользуется смартфонами, 81% — подключается к Интернету, 51% — использует высокотехнологичные устройства (то есть стоимостью свыше $500)» (Marie Gillespie *et al*., *Mapping Refugee Media Journeys: Smartphones and Social Media Networks*: *Research Report*, Open University and France Médias Monde, 13 May 2016, доступно по адресу: www.open.ac.uk/ccig/research/projects/mapping-refugee-media-journeys).

59 Ibid.

60 Ibid., p. 13. В исследовании подчеркивается: «Необходимо особо отметить, что в ходе интервью с беженцами вопросам доверия и конфиденциальности уделялось огромное внимание. Страх стать объектом слежки со стороны не только французских властей, но даже и других беженцев, страх, что окружающие узнают, что ты беженец, были ключевым камнем преткновения, когда они отвечали на вопросы во время интервью или неформальных бесед за рамками собственно интервью» (ibid., p. 43).

61 Ibid., p. 17.

что там нет такой слежки, как в Twitter и Facebook»[62]. Недоверие как к органам власти, так и к учреждениям и организациям у них на финансировании толкает беженцев в объятия «неофициальных, потенциально опасных и эксплуататорских структур»[63]. Получатели помощи, находящиеся вдали от военизированных границ так называемой «крепости Европа» и незнакомые с понятием «защиты данных», также выражали серьезные опасения, что различные акторы могут использовать информацию в ущерб их интересам[64].

Но риски «пособничества слежке» на этом не заканчиваются. Отдельные документы, которые разоблачитель Эдвард Сноуден передал журналистам в 2013 г., показывают, что ГО были мишенью слежки Агентства национальной безопасности и Центра правительственной связи — ключевых учреждений слежки и разведки США и Великобритании. Они перехватывали сообщения сотрудников Детского фонда ООН, Программы развития ООН, «Врачей без границ»[65] и других. Вполне можно предположить, если этим занимаются Великобритания и США, то и другие внутригосударственные и иностранные разведслужбы по мере своих возможностей следят за ГО, что также порождает серьезные последствия для деятельности самих ГО и получателей помощи. Те, кто безразличен к массовой слежке, считая, что «так уж устроен мир», наивно успокаивают себя мыслью, что она носит в основном пассивный характер, то есть что это просто слежка ради слежки, однако понятно, что различные силы в погоне за политическим или военным превосходством всегда готовы помешать работе ГО. Сюда можно включить, например, поиск целей или живой силы противника, сбор разведданных о месте их нахождения, манипулирование гражданским населением или же создание препятствий распределению гуманитарной помощи. Более того, даже понимая риски, связанные с обменом персональными дан-

62 G. Hosein and C. Nyst (примечание 29 выше), p. 48.

63 Ibid., pp. 13–18. Нужно также принять во внимание предложение Европейской службы пограничной и береговой охраны Фронтекс (FRONTEX) разработать приложение для смартфонов, чтобы обеспечить безопасность людей, пересекающих Средиземное море. Организации, защищающие права мигрантов и конфиденциальность, указывали, что беженцам, несомненно, не понравится приложение, упрощающее правительствам европейских стран слежку за ними и их перехват (см.: Diane Taylor and Emma Graham-Harrison, "EU Asks Tech Firms to Pitch Refugee-Tracking Systems", *The Guardian*, 18 February 2016, доступно по адресу: www.theguardian.com/world/2016/feb/18/eu-asks-tech-firms-to-pitch-refugee-tracking-systems).

64 Результаты неопубликованного исследования автора, которое он провел в 2015 г. в секторе Газа (имеется в распоряжении автора), говорят о серьезных сомнениях в надежности защиты персональных данных, поскольку люди разочарованы международными неправительственными организациями и международными организациями, которые проводили там исследования и фиксировали персональные данные, включая имена и фамилии, а также собирали удостоверения личности, которые так и не вернули. В свою очередь это недовольство породило подозрения местных жителей, которые все меньше верят намерениям подобных организаций.

65 См.: James Ball and Nick Hopkins, "GCHQ and NSA Targeted Charities, Germans, Israeli PM and EU Chief", *The Guardian*, 20 December 2013, доступно по адресу: www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner. См. также: Joan Tilouine and Simon Piel, "British Tapped UN and NGO Phones and Emails in Nigeria and Congo", *Le Monde*, 8 December 2016, доступно по адресу: www.lemonde.fr/afrique/article/2016/12/08/british-tapped-un-and-ngo-phones-and-emails-in-nigeria-and-congo_5045681_3212.html.

ными, люди намного хуже понимают, какие риски порождают сбор «метаданных» и слежка[66]. Это, в свою очередь, ставит важные вопросы, в какой степени ГО, использующие новые технологии при оказании гуманитарной помощи, должны сознавать присущие им риски, и обязаны ли ГО предупреждать о них получателей помощи во исполнение своего мандата предоставлять им защиту.

Сотрудники Международного Комитета Красного Креста (МККК) в числе других уже сейчас призывают принять совместные меры против подобных угроз. В качестве предупреждения об опасности хакерских атак со стороны органов власти и негосударственных акторов в 2016 г. на странице блога МККК появился пост, где приведен гипотетический, но уже хорошо знакомый пример онлайн-платформы ГО для краудсорсинга в реальном времени сведений о необходимой гуманитарной помощи и свидетельств о нарушениях прав человека. Автор предложил представить, что будет, если кто-то тайно взломает или подменит эту платформу, чтобы создать ложное представление о том, кто же на кого напал[67]. «Успешная хакерская атака может быстро изменить восприятие и ход вооруженного конфликта», — говорилось в посте[68]. Учитывая физические нападения на ГО, начиная с их санитарных колонн, учреждений и вплоть до персонала, автор также утверждал, что «правила меняются, а репутация нейтральной организации уже не гарантирует защиты»[69]. В этом случае «прямые нападки на репутацию организации могут стать все более подходящим способом… распространять ложную информацию о ее мандате, результатах и целях ее работы или намерениях ее сотрудников»[70]. И без слов ясно, что это может привести к катастрофическим последствиям как для сотрудников организации, их безопасности и репутации, так и для получателей помощи.

В феврале 2017 г. президент Майкрософт Брэд Смит призвал заключить пятую «цифровую Женевскую конвенцию», чтобы защитить в Интернете гражданских лиц и остановить тревожный рост числа кибератак, за которыми стоят органы власти, компьютерных взломов государственных учреждений в мирное время, а также повышение потенциала наступательных войн в киберпространстве и превращение программного обеспечения в оружие для решения задач национальной безопасности[71]. И хотя эта идея получила некую поддержку в гуманитарных кругах, все

66 *Метаданные* — это данные о данных. Телекоммуникационные метаданные включают время и длительность телефонных звонков, номер абонента и номер того, кому он звонил, отправлял электронные и мгновенные сообщения и другие виды электронных сообщений. Эту информацию можно использовать, чтобы составить подробное представление о месте нахождения человека, его передвижениях и контактах.

67 A. Kaspersen and C. Lindsey-Curtet (примечание 1 выше).

68 Ibid.

69 Ibid.

70 Ibid.

71 См.: Brad Smith, "The Need for a Digital Geneva Convention", *Microsoft Blog*, 14 February 2017, доступно по адресу: blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention.

свелось лишь к мелким изменениям тех программ массовой слежки, которые разоблачил Эдвард Сноуден, а вызывающая тревогу роль фактических пособников этих программ, которую взяли на себя многие технологические компании, дает основание полагать, что в этой войне быстрой победы не одержать[72].

Защита данных в гуманитарной деятельности

Организация «Прайваси Интернэшнл», основываясь на результатах своих прошлых исследований в области конфиденциальности, оказания помощи и развития, в докладе «Пособничество слежке» резко изменила отношение к поддержке повсеместного внедрения технологий, что по вполне понятным причинам в то время преобладало в секторе оказания помощи и развития[73], и заложила фундамент более общей дискуссии о важности защиты данных в гуманитарной деятельности. В период с 2013 по 2016 г. такие организации, как «Врачи без границ», «Партнерство в обучении оказанию денежной помощи» (Cash Assistance Learning Partnership), УКГВ, Оксфам, Управление Верховного комиссара ООН по делам беженцев (УВКБ), Всемирная продовольственная программа ООН, инициатива ООН «Глобальный пульс» и МККК ввели в действие внутренние правила защиты и передачи персональных данных либо публично обязались ответственно использовать эти данные[74].

В 2015 г. на Международной конференции комиссаров по защите персональных данных и конфиденциальности была впервые принята резолюция «Конфиденциальность и международная гуманитарная деятельность». В ней подчеркивалось, что обработка данных изначально присуща миссии гуманитарных организаций, но «в целом гуманитарное сообщество все еще не принимает достаточных мер» для внедрения нормативной базы по защите данных[75]. Резолюция также осветила некоторые ключевые проблемы соблюдения юридических норм и принципов защиты данных, с которыми сталкиваются ГО. К ним относится сбор «конфиденциальных данных» (их определение недавно появилось в Общем регламенте ЕС в отношении защиты данных (ОРЗД): «…персональные данные, по которым можно установить расовое или этническое происхождение человека, его политические предпочтения, религиозные или философские убеждения, членство в профсоюзах, сведения о состоянии здоровья, сексуальной жизни и сексуальной

72 См.: Ian Brown, Mort Halperin, Ben Hayes, Ben Scott and Mathias Vermeulen, "Towards Multilateral Standards for Surveillance Reform", in Russell Miller (ed.), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*, Cambridge University Press, Cambridge, 2017.

73 См.: Kristin Bergtora Sandvik and Maria Gabrielsen Jumbert (eds), *The Good Drone*, Routledge, London, 2017.

74 См.: Jos Berens, Ulrich Mans and Stefaan Verhulst, *Mapping and Comparing Responsible Data Approaches*, GovLab and Leiden University Centre for Innovation, June 2016, pp. 5–6.

75 37th International Conference of Data Protection and Privacy Commissioners, "Resolution on Privacy and International Humanitarian Action", Amsterdam, 27 October 2015 (далее — ICDPPC Resolution).

ориентации, генетические данные и биометрические данные»), что запрещено, если не соблюдаются строгие условия и требования[76].

На конференции также говорилось, что системы мониторинга и управления информацией, электронная пересылка данных, системы идентификации и биометрии, приложения для мобильных телефонов и дроны, а в сущности и вся совокупность инноваций в сфере гуманитарной деятельности «порождают особые угрозы конфиденциальности и безопасности»[77]. В резолюции конференции прозвучало предупреждение, что «на гуманитарные организации, не пользующиеся привилегиями и иммунитетом, может оказываться давление, чтобы они предоставили органам власти сведения, собранные в гуманитарных целях, для их последующего использования в иных целях (например, для контроля миграционных потоков и борьбы с терроризмом)»[78]. Несмотря на отмеченные в резолюции многочисленные риски, которые несет для ГО обработка данных, и прозвучавший в ней призыв соблюдать международные нормы в области защиты данных, там практически ничего не говорится о том, как же на практике преодолеть те особые и во многом уникальные трудности, с которыми сталкивается сектор. Это же относится и к множеству нормативных документов о защите данных, принятых ГО. Хотя в них отразились ключевые принципы защиты данных, там зачастую отсутствуют четкие процедуры, позволяющие претворить их в жизнь в затруднительных обстоятельствах гуманитарной деятельности. В июле 2017 г. МККК и Брюссельский центр конфиденциальности сделали большой рывок и ликвидировали этот пробел, опубликовав «Руководство по защите данных в ходе гуманитарной работы (Руководство МККК)»[79].

Далее в статье будут рассмотрены некоторые ключевые и общие для всего сектора проблемы на основе главных тем, освещенных в Руководстве МККК. В анализе для примера и сравнения взяты за основу нормы защиты данных, содержащиеся в ОРЗД ЕС. Когда в анализе упоминаются «законы о защите данных», это в широком смысле относится к принципам, общим для национальных и международных нормативно-правовых баз[80].

76 ОРЗД (примечание 48 выше), ст. 9. В резолюции Международной конференции комиссаров по защите персональных данных (примечание 75 выше) также отмечено, что «данные, которые обычно законами по защите данных не относятся к конфиденциальным, могут в значительной степени приобрести эти качества в гуманитарном контексте чрезвычайного характера». ОРЗД является законом ЕС, в то время как резолюция Международной конференции комиссаров по защите персональных данных — рекомендательная мера «мягкого права».

77 ICDPPC Resolution (примечание 75 выше).

78 Ibid.

79 Christopher Kuner and Massimo Marelli (eds), *Handbook on Data Protection in Humanitarian Action*, ICRC, Geneva, 2017 (далее — ICRC Handbook).

80 В них входят нормативно-правовые базы, разработанные ООН (резолюция ГА ООН «Руководящие принципы регламентации компьютеризированных картотек, содержащих данные личного характера» от 14 декабря 1990 г., документ ООН A/Res/45/95), Советом Европы (Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера от 28 января 1981 г.) (вступила в силу 1 октября 1985 г.); Рекомендации Комитета министров № R (99) 5 «Защита конфиденциальности в Интернете: Руководство по защите физических лиц при сборе и обработке персональных данных в информационных магистралях» от 23 февраля 1999 г.; Дополнительный протокол к Конвенции о защите частных лиц в отношении автомати-

В статье уделяется особое внимание ОРЗД по нескольким причинам. Во-первых, соотнесение проблем в сфере защиты данных с юридическими нормами защиты данных требует некоей исходной точки, и при отсутствии сравнимых международных законов или конвенций более широкого охвата был выбран закон ЕС, так как он общепризнанно считается «золотым стандартом». Более того, распространение законов о защите данных неуклонно продолжается по всему миру, и вполне вероятно, что ЕС будет и далее устанавливать стандарты в этой области. Во-вторых, ОРЗД — первый закон о защите данных, в котором конкретно, хотя и вскользь, упоминается гуманитарная деятельность[81]. В-третьих, даже если ГО работают в странах, где данные слабо защищены законом, им в любом случае придется соблюдать нормы ОРЗД, если их штаб-квартира находится на территории ЕС или если они намерены вести там какую-либо деятельность или передавать туда данные. Даже пользующимся привилегиями или иммунитетом организациям, которые до сих пор считали, что эти законы не имеют отношения к их работе и документам, чем дальше, тем больше придется готовиться доказывать наличие у них адекватных механизмов защиты данных, если они намерены получать их от органов власти или ГО стран — членов ЕС[82]. В-четвертых, в информационный век защита данных стала центральным элементом защиты основных прав, поэтому считается, что ГО как часть сообщества, преданного делу защиты прав человека, должны стремиться в этом к высочайшим стандартам.

Законность обработки данных

Законы о защите данных устанавливают «правовые основания» или допустимые «условия обработки» данных, что автоматически лишает ГО или любых иных операторов данных законных прав обрабатывать персональ-

зированной обработки данных личного характера, касающийся надзорных органов и трансграничных потоков данных от 28 ноября 2001 г.; Руководство по защите частных лиц в отношении автоматизированной обработки данных личного характера в мире больших данных от 23 января 2017 г., разработанное Консультативным комитетом Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера). А также разработанные Европейским союзом (Директива Европейского парламента и Совета Европейского союза № 95/46/ЕС от 24 октября 1995 г. «Защита прав частных лиц применительно к обработке данных личного характера и о свободном движении таких данных»), Организацией экономического сотрудничества и развития («Руководство по защите конфиденциальности и трансграничных потоках персональных данных» от 23 сентября 1980 г.), Организацией Азиатско-Тихоокеанского экономического сотрудничества («Нормативно-правовая база АТЭС в сфере конфиденциальности», 2004 г.) и Экономическим сообществом западноафриканских государств (Дополнительный закон ЭКОВАС о защите персональных данных от 16 февраля 2010 г.).

81 ОРЗД (примечание 46 выше), преамбула, пп. 46, 73, 112.

82 Нормы ОРЗД разрешают передавать данные за пределы ЕС лишь в те страны, в отношении которых было принято «адекватное решение» (это значит, что в этой стране действуют сравнимые стандарты защиты данных), или тем получателям, которые связаны обязательными нормами защиты данных, либо предусмотренными стандартными условиями контракта, которые установила Европейская комиссия, либо корпоративными нормами, которые утвердил надзорный орган в области защиты данных (там же, ст. 44–48).

ные данные без такого правового основания[83]. В списке таких оснований на первом месте стоит согласие, и на него ГО традиционно полагались, как на фундамент своей собственной деятельности по сбору данных. Однако работа многих ГО ставит вопросы: всегда ли условия его получения отвечали нормам, которые требуют «добровольного», «однозначного» и «информированного согласия?»[84] Причина здесь в том, что нуждающимся в гуманитарной помощи людям, если они хотят получить ее, зачастую (хотя и не всегда) не остается иного выбора как только зарегистрироваться и предоставить свои данные. Более того, субъектов данных необходимо проинформировать, каким образом будут использованы их данные, кому и зачем они будут передаваться, а их согласие на это необходимо задокументировать. Однако информировать людей об этом и получать их согласие — достаточно трудная задача, учитывая, как много ГО зачастую участвует в распределении гуманитарной помощи для перемещенных внутри страны лиц или тех, кто заперт в осажденных городах, а также неимоверные трудности, порожденные уникальностью или масштабом чрезвычайных ситуаций, в которых работают ГО.

По этим причинам ГО могут решить обрабатывать данные на основании альтернативных правовых норм. Международные организации, действующие в соответствии с гуманитарными мандатами, обусловленными международным правом, могут решить обрабатывать персональные данные, следуя им, но для неправительственных организаций это не выход. ОРЗД ЕС косвенно рекомендует ГО при обработке данных руководствоваться «жизненными интересами» субъектов данных[85], но также утверждает, что случаи такой обработки данных возможны только тогда, когда «она не может быть осуществлена на ином правовом основании»[86]. Кроме того, «конфиденциальные данные» могут очень быстро оказаться необходимыми для доступа к службам жизнеобеспечения, а их обработка без согласия владельца допускается, если только он физически или юридически не способен дать на это согласие либо в рамках соблюдения законов об охране здоровья или о чрезвычайных ситуациях[87]. Из-за подобных нестыковок ГО вынуждены при-

83 Нормы ЕС, например, относят к законной только такую обработку данных, которая основана на согласии субъекта данных, — для исполнения договора или выполнения правового обязательства; для защиты жизненно важных интересов субъекта данных или другого лица; для выполнения задачи в публичных интересах или в рамках осуществления государственной власти; для целей, вытекающих из легитимных интересов оператора данных или третьего лица, за исключением случаев, когда преимущество над такими интересами имеют интересы или фундаментальные права и свободы субъекта данных, требующие защиты персональных данных. О законности обработки данных см. там же, ст. 6.

84 Нормы ЕС определяют «согласие» как ясное подтверждение «свободно данного конкретного и сознательного указания о своей воле, которым субъект данных оповещает о своем согласии на обработку касающихся его персональных данных» (там же, преамбула, п. 32).

85 Там же, преамбула, п. 46.

86 Там же.

87 В гуманитарном контексте обстоятельства, когда субъекты данных могут быть лишены возможности выразить свое согласие, включают ситуации, когда невозможно дать субъекту данных требуемую информацию об обработке данных, когда субъект данных может не понять всю сложность самого процесса их обработки и когда возникает существенно неравное соотно-

нимать непростые решения: когда согласие необходимо, а когда нет, и как осуществить достаточно строгие (и прописанные в законе) процедуры, чтобы его получить и задокументировать. Тем же ГО, которые решат обрабатывать данные, основываясь на «жизненно важном интересе» получателей помощи (по определению это «интерес, который важен для выживания субъекта»), также придется подтверждать, что такая обработка необходима и соразмерна (то есть не избыточна) этим целям[88]. Полагающимся на согласие ГО также придется соблюдать более строгие нормы в отношении детей (для них нормой является согласие родителей) и на практике следовать нормам отказа от согласия, при этом данный процесс не должен быть сложнее, чем его получение. И всем ГО придется оказывать содействие субъектам данных в соблюдении их права оспорить обработку их данных и в надлежащих случаях исправлять или уничтожать их.

Прозрачность для получателей помощи

Прозрачность лежит в основе защиты данных, она должна стать второй натурой тех ГО, которые обязались отвечать за свою работу перед пострадавшими людьми. Вне зависимости от правовой основы обработки данных законы о защите данных требуют от операторов, чтобы процесс их обработки был прозрачным для субъектов данных[89]. И речь идет не только об информированном согласии — законы о защите данных дают субъектам данных право на всю такую информацию[90]. Согласно нормам ОРЗД они «должны быть осведомлены о рисках, правилах, средствах защиты и правах в отношении обработки персональных данных и о том, как реализовать свои права в связи с такой обработкой», при этом «конкретные цели обработки персональных данных должны быть ясными и законными и должны определяться в момент сбора персональных данных»[91]. Предоставление таких сведений получателям гуманитарной помощи сталкивается с очевидными сложностями, а на практике может быть трудно добиться применения даже минимума этих норм[92]. Хотя ГО имеют все правовые основания ссылаться на обстоятельства, которые при сборе данных затрудняют или исключают возможность информировать получателей помощи об их

шение сил оператора данных и их субъекта, и при этом последнему не предлагается никакой реальной альтернативы передачи собственных данных см.: ICRC Handbook (примечание 79 выше), ch. 3.

88 ЕС определяет «жизненные интересы» как те, которые «жизненно важны для субъекта данных или иного физического лица» (ОРЗД (примечание 48 выше), преамбула, п. 46). В подразделе 3.3. Руководства МККК (ICRC Handbook, примечание 79 выше) предлагается более широкая интерпретация.

89 Например, ОРЗД (примечание 48 выше), ст. 12–22, 34.

90 Там же.

91 Там же, преамбула, п. 39.

92 Согласно нормам ОРЗД, «до физических лиц должно быть прозрачно донесено то, что их персональные данные собираются, используются, просматриваются или иным образом обрабатываются, а также то, в каком объеме персональные данные обрабатываются или будут обрабатываться».

обработке, однако они не могут полностью игнорировать эти требования, оправдываясь острой необходимостью в какой-либо особой ситуации. Вместо этого они должны задействовать новые способы довести информацию до получателей помощи, включая информационные кампании постфактум, вернуться к вопросам защиты данных и включить их в программы индивидуального консультирования и работы с населением, они также могут задействовать справочные службы и ИКТ в помощь тем, кто ищет эту информацию.

Такие методы особенно применимы в ситуациях, когда ГО собирают данные, не зная точно, как они будут использованы или кому будут переданы, например в ходе опросов населения и оценки факторов уязвимости перед началом операций по ликвидации последствий чрезвычайных ситуаций. Как уже говорилось, чтобы избежать «расползания функций» (постепенного расширения сферы применения технологий или систем за пределы их изначального предназначения), законы о защите данных обычно требуют, чтобы операторы при сборе данных указывали, в каких целях они будут потом использованы[93]. Проблемы ГО в том, что они должны, с одной стороны, говорить максимально конкретно, а с другой стороны, гибко использовать данные и в тех целях, которые могут только возникнуть по мере разворачивания гуманитарных операций и расширения их масштабов. Если же цели сбора данных и (или) состав партнеров ГО значительно изменились, они могут быть обязаны проинформировать об этом получателей помощи и заручиться новым или дополнительным согласием субъектов данных — в зависимости от того, как было получено первоначальное согласие. В этом случае им предстоит еще одна трудная задача: решить, где же здесь проходит разделительная черта. Общее согласие, дающее ГО карт-бланш на любую необходимую им обработку данных получателей помощи без последующих консультаций с ними, прямо нарушает основные принципы защиты данных, однако получение дополнительного разрешения на новую обработку данных неизбежно связано со значительными логистическими, оперативными и материальными трудностями. Ключевая проверка на правомерность обработки — выяснить, соответствует ли она «целям, для которых персональные данные были изначально собраны»[94]. Но если целью считается оказание «гуманитарной помощи», то здесь ГО могут действовать свободнее других операторов данных[95].

Информационная безопасность

Беженцам, лицам, ищущим убежища, и перемещенным внутри страны лицам грозит множество опасностей; они исходят от стран их происхождения, стран пребывания, транзита и назначения (если в них действует репрессивная политика изоляции), от враждебных третьих сторон, в том

93 ОРЗД, например, там же, ст. 13.
94 Там же, ст. 6(4).
95 ICRC Handbook (примечание 79 выше), subsection 2.6.3.

числе, например, негосударственных вооруженных формирований, преступников и даже «хактивистов» (использующих подрывные возможности ИКТ в политических целях или стремящихся добиться изменений в обществе). Все они потенциально опасны, так как могут использовать персональные данные во вред законным интересам людей, подвергнуть серьезной опасности некие группы или отдельных людей либо значительно подорвать способности ГО выполнять свой мандат. Собранные у получателей помощи данные будут надежно защищены только при соблюдении строгих норм и практических мер информационной безопасности, которые для ГО и беспомощных людей по существу являются единственной защитой от потенциальных недоброжелателей.

Работа на местах и вообще небезопасна, но с появлением ИКТ переход с физических носителей на цифровые породил в гуманитарном секторе новый комплекс проблем. Как правило, из-за недостатка технических знаний на местах разработчики локальных баз данных, решений и инноваций, сыгравших неоценимую роль в предоставлении защиты и оказании помощи, не всегда, мягко говоря, руководствовались требованиями информационной безопасности. И хотя централизованные базы данных должны быть намного лучше защищены, потенциальная необходимость открыть доступ к ним широкому кругу пользователей создает проблемы иного рода. Именно пользователи ИКТ, как и в иных больших организациях, являются самым слабым звеном в ГО. Многие не обучены даже основам информационной безопасности и, как и большинство пользователей ИКТ, то и дело действуют в ущерб как личной безопасности, так и безопасности своей организации[96].

Это важно учитывать потому, что успех огромного большинства компьютерных взломов обусловлен не наличием внутренних технических изъянов (как в случае обхода брандмауэров, взлома баз данных), а некоей формой «социальной инженерии» или психологических манипуляций. Например, пользователей или сотрудников обманом вынуждают переслать конфиденциальные или служебные данные простым нажатием на фиктивную ссылку или открыть приложение к электронному письму с вредоносным кодом (специально созданным, чтобы нарушить работу компьютерной системы, повредить ее либо получить к ней доступ). Растет количество таких взломов и уровень их сложности[97], поэтому для ГО на местах меры информационной безопасности должны стать неотъемлемой частью общих мер безопасности, а сотрудников нужно надлежащим образом обучать их соблюдать. Следование нормам информационной безопасности уже вошло в привычку у коммерческих компаний, защищающих свои активы и репу-

96 См.: Fran Howarth, "The Role of Human Error in Successful Security Attacks", *IBM SecurityIntelligence*, 2 September 2014, доступно по адресу: securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/.

97 Symantec, "Extraordinary Attacks, High-Dollar Heists, Electoral Disruption", *2017 Internet Security Threat Report*, ISTR 22, April 2017.

тацию, но гуманитарным организациям еще предстоит пережить этот необходимый культурный сдвиг[98].

Как ни банально это иногда звучит, но простейший способ защитить данные — вообще не собирать их или же как минимум собирать только необходимые. Следующий наилучший вариант — проверить правильность и актуальность данных и уничтожить те, в которых больше нет нужды. Эти принципы воплощены в понятиях «указания цели», «необходимость и соразмерность» и «минимизация данных»[99], однако различные настоятельные потребности гуманитарного сектора толкают его в противоположном направлении. Кажется, что изначально многие ГО по умолчанию исходят из того, что персональные данные нужно хранить неопределенно долго, если не вечно, чтобы соответствовать требованиям аудита[100]. Раздутые утверждения о возможностях больших данных (см. ниже) также поощряют ГО собирать и хранить больше персональных данных, чем требуется. Во многих ГО плохо организована «цифровая гигиена», из-за чего у них остаются следы этих данных, что повышает риски для получателей помощи, хотя ГО следовало бы свести к минимуму и ограничить доступ к данным, правомерно хранящимся в архиве. Для решения этих проблем необходим еще один культурный сдвиг.

С архивным хранением документов о гуманитарной деятельности связан отдельный комплекс проблем защиты данных. Множество убедительных причин (некоторые содержатся в их мандатах) заставляет определенные ГО хранить подробные архивы о своей деятельности хотя бы потому, что эта информация может в будущем оказаться критически важной для субъектов данных, например беженцев и их родственников. Трудность состоит в том, как совместить сохранение «гуманитарной памяти» с соблюдением основных принципов защиты данных. К примеру, в УВКБ ООН уже давно действует политика в отношении документов и архивов, согласно которой личные дела получателей помощи должны храниться неопределенно долго, хотя новая политика защиты данных требует уничтожать пер-

98 В недавнем докладе о том, как гуманитарные акторы справляются с подобными рисками, утверждается: «С точки зрения времени сотрудников и уделяемого внимания приоритетом является управление рисками безопасности, сразу же за ним следует управление финансовыми рисками (профилактика мошенничества и нецелевого использования средств)... Исследование показало, что подход на основе управления риском пользуется меньшим вниманием и пониманием в сфере информационной безопасности и соблюдения законодательных норм (например, норм антитеррористического законодательства)» (Abby Stoddard, Katherine Haver and Monica Czwarno, *NGOs and Risk: How International Humanitarian Actors Manage Uncertainty*, Humanitarian Outcomes and InterAction, February 2016, доступно по адресу: https://www.humanitarianoutcomes.org/publications/ngos-and-risk-how-international-humanitarian-actors-manage-uncertainty).

99 Эти принципы содержатся во многих законах о защите данных. Например, см.: ОРЗД (примечание 48 выше), ст. 5(1)(b) об указании цели и ст. 5(1)(c) о необходимости, соразмерности и минимизации данных.

100 Кажется, что многие ГО, в ожидании внутреннего и внешнего аудита программ со стороны органов власти и доноров, боятся уничтожать данные, при этом может оказаться затратным и сам процесс выбора: какие данные сохранить, от каких избавиться, а какие — надежным образом уничтожить.

сональные данные, как только в них пропадает необходимость[101]. Однако сегодня все персональные данные получателей помощи УВКБ считаются составной частью их личных дел, и, вопреки нормам защиты данных самой организации, все они подлежат бессрочному хранению. Понятен общественный и частный интерес сохранить исторические документы о беженцах, но так ли необходимо хранить в архивах все до последней подробности о пребывании человека в лагере беженцев, особенно с учетом все растущего объема накопленных данных? А вдруг в будущем кто-то возразит против хранения какого-либо документа в своем личном деле и потребует удалить его, сославшись на свои основные права? Автономность лежит в основе защиты данных, но патернализм изначально присущ гуманитаризму, и между ними необходимо найти золотую середину.

Обмен и забота

Многие ГО в целях содействия программам защиты и помощи или их расширения делятся персональными данными с третьими сторонами, в том числе с органами власти страны пребывания, оперативными партнерами и (или) партнерами по реализации программ, коммерческими поставщиками услуг. Хотя интуиция сторонников конфиденциальности и защиты данных говорит им об обратном, важно подчеркнуть, что объединение сведений, собранных всеми ГО, которые пришли на помощь перемещенным внутри страны людям, не только жизненно важно для ликвидации последствий чрезвычайных ситуаций, но и позволяет, по сути, снизить сопутствующие риски, так как значительно сокращает объем собранных и хранимых данных. Одновременно заметно падает «усталость от опросов», на что часто жалуются нуждающиеся в помощи люди, которым без необходимости раз за разом приходится отвечать на вопросы о том, какая же именно помощь им необходима. Однако пока весь сектор не станет придерживаться одинаковых стандартов защиты данных, такое сотрудничество будет порождать множество практических проблем, а конкуренция за финансирование среди ГО, их пересекающиеся мандаты и политические вопросы принадлежности данных лишь существенно осложнят их. ГО также необходимо более ответственно подойти к своей роли «привратников», охраняющих конфиденциальную информацию, в ответ на повышенное внимание к ним СМИ, исследовательских организаций и частных компаний. Добиваясь положительного освещения проблемы беженцев или помогая исследователям, которые обещают лучше понять проблемы беженцев и выяснить, в какой помощи они нуждаются, ГО могут не всегда учитывать свои правовые обязательства или этическую подоплеку своих действий[102].

101 См. положения о хранении данных: УВКБ ООН, Политика в отношении защиты персональных данных лиц, подмандатных УВКБ ООН, май 2015 г., ст. 4(6).

102 См.: European Commission, "Guidance Note — Research on Refugees, Asylum Seekers & Migrants", Directorate-General for Research and Innovation, доступно по адресу: ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-refugees-migrants_en.pdf.

Нормы законов о защите данных требуют, чтобы субъекты данных явно выразили согласие на передачу данных другой организации[103]. Операторы данных также обязаны проверять, способны ли все сторонние получатели данных обеспечить их надлежащую защиту, будут ли они использовать их только в заявленных целях и передавать только те данные, которые необходимы для достижения этих целей. Передача данных должна регламентироваться юридическими или договорными соглашениями, осуществляться по защищенным каналам связи, но в ГО вся предыдущая практика обмена данными, как правило, очень далека от соблюдения этих требований[104]. Субъекты данных также должны иметь возможность пользоваться своими правами, получать и добиваться получения компенсаций, если им был нанесен ущерб. Для формализации механизмов обмена данными, как того требуют минимальные стандарты их защиты, необходимо кардинально изменить практические подходы на местах, но эти трудности преодолимы. Например, в УВКБ ООН была проведена тщательная оценка влияния мероприятий по защите данных на программу по переводу наличных средств. В результате были разработаны инновационные процедуры систематизации механизмов обмена данных, оценки адекватности систем защиты данных третьих сторон, минимизации передаваемых данных и заключения соглашений об обмене данными с широким кругом партнеров[105].

Природа и степень рисков, связанных с обменом данными, конечно же, сильно зависят от типа данных и получателя. Поэтому можно считать, что обмен данными с оперативными партнерами или поставщиками услуг, которые следуют строгим нормам собственной политики защиты данных, не представляет особых рисков. Однако сотрудничество с органами власти, чья политика в отношении мигрантов и беженцев (или отдельных религиозных или этнических групп) может со временем измениться, зачастую

103 Эти положения в общем применяются только к ситуациям, когда получатель данных будет контролировать их использование. Соблюдая определенные меры предосторожности, организации могут передавать данные субподрядчикам на обработку в собственных интересах или под собственным руководством (см., например: ОРЗД (примечание 48 выше), ст. 6(1), 7, 28).

104 См., например, рекомендации доклада о результатах оценки влияния мероприятий по защите данных для УКВБ ООН: «…передача данных, по которым можно установить личность беженцев, в составе незашифрованных документов или на носителях, которые могут быть утеряны или похищены, должна быть сведена к абсолютному минимуму. Там, где это возможно, практика пересылки таких документов по электронной почте должна быть заменена передачей их по безопасным каналам FTP или через VPN. Если документы будут отправляться по электронной почте, необходимо прекратить практику отправки паролей к зашифрованным файлам вслед за самими файлами и заменить ее более защищенными процедурами. Целью в среднесрочной перспективе должно стать внедрение защищенных систем ИКТ, которые не только позволят партнерам УВКБ ООН пользоваться его данными (а также исправлять и дополнять их), но и существенно повысят возможности УВКБ ООН контролировать их» (UNHCR and Trilateral Research & Consulting, *Privacy Impact Assessment of UNHCR Cash Based Interventions*, Geneva, December 2015, p. 23, доступно по адресу: www.globalprotectioncluster.org/_assets/files/tools_and_guidance/cash-based-interventions/erc-privacy-impact-assessment-of-unhcr-cbi_en.pdf).

105 Ibid.; см. также: UNHCR, *Operational Guidelines on the Protection of Personal Data of Persons of Concern*, 2018.

считается весьма рискованным[106]. Чтобы лучше ориентироваться в подобных обстоятельствах, ГО крайне важно оценить адекватно правовую базу, в рамках которой работают их партнеры и поставщики услуг на местах, и проанализировать действующие законы сквозь призму того ущерба, который ГО могут причинить собственным получателям помощи. Часто такая оценка выявляет разного рода обязательства разглашать информацию, о чем шла речь выше; сегодня это происходит повсеместно, что, как правило, порождает риски несоблюдения или нарушения основных прав получателей гуманитарной помощи. Некоторые риски очевидны, например связанные с требованием информировать органы власти о носителях таких «расстройств», как СПИД, туберкулез и даже гомосексуальность. Хотя ГО могут придерживаться принципиальной позиции о соблюдении подобных правовых норм и зачастую так и происходит, но их партнеры на местах порой оказываются в ином положении. Нередко риски совсем не очевидны, например порожденные правовыми нормами по борьбе с международным терроризмом или по противодействию отмыванию денег, так как они требуют, чтобы все поставщики финансовых услуг принимали меры «должной осмотрительности», осуществляя денежные переводы, и проверяли благонадежность владельцев банковских счетов[107]. Эти меры включают и проверку клиентов по сотням национальных и международных санкционных списков. Зачастую такая проверка поручается специализированным поставщикам услуг, а органы финансовой разведки и национальной безопасности страны следят за этим процессом. Растет понимание важности защиты данных в секторе наличного оборота денег, как и число ГО, занятых в программах денежной помощи. Однако совсем не очевидно, что эти ГО осознают необходимость прямо поставить вопрос защиты данных перед своими поставщиками услуг[108]. Многие санкционные списки вводятся странами, которые либо являются стороной в конфликте, либо имеют иное отношение к вооруженным столкновениям, поэтому перевод наличных средств через их банки может невольно подорвать нейтральный статус ГО, так как они втягиваются в мероприятия по применению санкций.

Похожую проблему порождают и условия регистрации клиентов компаний мобильной связи, и условия хранения их данных. При этом поставщики услуг нередко обязаны хранить сведения о клиентах, об их телефонных разговорах и даже их содержание и передавать такие сведения в распоряжение правоохранительных органов и служб безопасности.

106 Например, УВКБ ООН часто обязано делиться биографическими данными беженцев, зарегистрированных в стране пребывания, и при этом мало что может сделать для их защиты, кроме как постараться сократить до минимума передаваемую информацию.

107 См.: Gavin Sullivan and Ben Hayes, *Blacklisted: Targeted Sanctions, Pre-emptive Security and Fundamental Rights*, European Centre for Constitutional and Human Rights, Berlin, 2011. См. также: Ben Hayes *et al.*, "*De-risking*"*: From Financial Surveillance to Financial Exclusion? Banking Problems and Solutions for the Non-Profit Sector*, Human Security Collective and Open Society Foundations, 2018.

108 См.: Jessica Burniske, Naz Modirzadeh and Dustin Lewis, "Counter-Terrorism Laws: What Aid Agencies Need to Know", Overseas Development Institute, Humanitarian Practice Network Briefing Paper No. 79, November 2014.

До появления мобильных телефонов подобные данные зачастую можно было получить, только если судья выписывал ордер телефонной компании, сегодня же может потребоваться лишь номер мобильного телефона. Тот факт, что слежка стала повсеместной и от нее все труднее избавиться, никак не освобождает ГО от обязанностей защищать данные. Даже наоборот — им настоятельно необходимо учитывать, что их сообщения получателям помощи, например массовую рассылку SMS, могут одинаково легко перехватить и органы власти, и негосударственные акторы. По возможности ГО необходимо пользоваться более безопасными альтернативными средствами связи, чтобы не скомпрометировать нейтральный характер своей гуманитарной деятельности и не нанести урон безопасности получателей помощи[109].

Выше отмечалось, что органы власти могут напрямую запросить данные у ГО или даже распространить на имеющиеся у них данные свою юрисдикцию, либо конфисковать их вопреки возражениям. В пользующихся привилегиями или иммунитетом организациях уже давно действуют устоявшиеся правила реагирования на запросы органов власти, и в ответ они могут привести различные законные причины отказа отвечать на необоснованные запросы, в том числе и ссылаясь на защиту основных прав получателей помощи[110]. Те же ГО, которые не пользуются подобной защитой и которые заранее не установили правила, помогающие в подобных ситуациях, рискуют причинить ущерб не только конфиденциальности получателей помощи, но и их защищенности и безопасности. В августе 2017 г. выяснилось, что министерство внутренних дел Великобритании, пытаясь найти и депортировать иностранцев, пользовалось базой данных Сводной информационной сети о бездомных, в которую благотворительные организации и правительственные учреждения страны направляют информацию о ночующих на улице бездомных, чтобы оказывать им адресную помощь[111]. Эта база данных принадлежит одной благотворительной организации помощи бездомным людям, в ней собрана информация об их местонахождении, гражданстве, психическом состоянии и гендерной

109 «Собирая данные о беженцах, необходимо найти золотую середину между требованиями безопасности и защиты общественного порядка, с одной стороны, и человеческим достоинством и соблюдением прав человека — с другой. И правительства, и учреждения по работе с беженцами, которым они передают свои данные, должны пользоваться их доверием. Технологические компании должны признать, что их платформы в одинаковой степени служат как беженцам, так и контрабандистам, и совершенствовать меры защиты пользователей, а нам следует задаться вопросом: что эти компании будут делать с данными, имеющими такое важное политическое значение» (Mark Latonero, "For Refugees, a Digital Passage to Europe", *Responsible Data Forum*, 8 February 2016, доступно по адресу: responsibledata.io/for-refugees-a-digital-passage-to-europe/).

110 См., например: UNHCR, *Guidelines on the Sharing of Information on Individual Cases:* "*Confidentiality Guidelines*", Geneva, August 2001. См. также: Els Debuf, "Tools to Do the Job: The ICRC's Legal Status, Privileges and Immunities", *International Review of the Red Cross*, Vol. 97, No. 897/898, 2016.

111 Mark Townsend, "Home Office Used Charity Data Map to Deport Rough Sleepers", *The Guardian*, 19 August 2017, доступно по адресу: www.theguardian.com/uk-news/2017/aug/19/home-office-secret-emails-data-homeless-eu-nationals.

принадлежности[112]. Это не единственный пример[113], все подобные случаи должны стать предостережением и иным организациям, которые ведут учет беспомощных и беззащитных людей или же снабжают других массивами «открытых данных» — такие данные могут быть использованы не в тех целях, для которых они изначально предназначались.

Большие данные

В знаменательном докладе Управления ООН по координации гуманитарных вопросов (УКГВ) 2013 г. отмечалось, что «найти способы сделать большие данные полезными для руководителей гуманитарных организаций — одна из величайших задач и возможностей сетевого века»[114]. Аргументы в защиту инноваций, возникающих в связи с большими данными в гуманитарном секторе, звучат особенно убедительно на фоне ситуаций, когда явные недостатки в области управления информацией снижают эффективность помощи и приводят к гибели людей. Нет сомнений в том, что такие инновации дают ГО шанс исправить некоторые свои фундаментальные недостатки и повысить эффективность своей работы, но безграничный оптимизм рассуждений УКГВ по поводу сопоставления и анализа «больших объемов информации, способных породить удивительно глубокое понимание обстановки в местах работы [ГО]», вообще не оставил места какой-либо защите данных[115].

Нужно признать, что нормы защиты данных и их относительно простые требования не очень-то вписываются в этот дивный новый мир, по крайней мере, на первый взгляд. Эти нормы требуют указывать цели сбора данных и ограничивать их, но технологии больших данных позволяют найти новое применение таким данным, встраивая их в системы «разумного интеллекта». Сами данные становятся смыслом сбора и обработки персональных данных, а «расползание функций» уже заложено в больших данных, потому что их предназначение — поиск нового применения дан-

112 St Mungo's, "CHAIN — Combined Homelessness and Information Network", доступно по адресу: www.mungos.org/work-with-us/chain/.

113 Можно привести еще примеры публикации самых актуальных данных о лицах, ищущих убежища, которые находятся в районе Африканского рога, их перемещениях и характеристиках. Такие данные могут невольно стать источником полезной информации для контрабандистов и торговцев людьми; информации о перемещениях беженцев во время вооруженного конфликта, которую в своих целях могут использовать стороны в вооруженном конфликте. Публикация географических карт, где показаны места проживания религиозных меньшинств или жертв сексуального насилия без учета соответствующих рисков, может причинить им еще больше вреда; публикация статистических данных о предоставлении помощи различным этническим, религиозным группам уже привела к обвинениям в предвзятости к ним. Первый приведенный пример описан в работе: Joseph Guay and Lisa Rudnick, "What the Digital Geneva Convention Means for the Future of Humanitarian Action", *UNHCR Innovation Service*, 25 June 2017, доступно по адресу: www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/. Последующие примеры основываются на опыте работы автора, они не отражены в публичных изданиях.

114 OCHA (примечание 54 выше), p. 26.

115 Ни на одной из 122 страниц этого документа УКГВ ни разу не появляется словосочетание «защита данных».

ных, о чем никто и не думал при их сборе. В свою очередь, большие данные стимулируют ГО применять все более сложные методики выявления получателей помощи и оценки того, в какой степени они нуждаются, чтобы оказывать помощь наиболее беспомощным и беззащитным. И все это вопреки неизбежному увеличению объемов данных (в том числе и конфиденциальных), которые придется собирать, чтобы получить характеристики отдельных людей, семей и домохозяйств. Из-за этих сложностей получателям помощи будет труднее понять свое участие (и они не смогут дать обдуманное согласие на него) в программах обработки больших данных. Особенно трудно им будет понять, каким образом информацию о них станут собирать, использовать, хранить, передавать третьим сторонам и анализировать. Важно и то, сбор всё больших объемов персональных данных для профилирования людей и последующей оценки всевозможных угроз, каким они могут подвергаться, также может не соответствовать их «жизненным интересам». Результаты применения методов анализа больших данных для оценки того, нуждаются ли те или иные люди в помощи, могут в результате привести к дискриминации, а лишившиеся помощи люди не сумеют оспорить эти результаты. И речь идет не только о правах отдельных людей — большие данные могут ущемить права сразу множества людей, отразиться на целых группах получателей помощи негативным или непредвиденным образом.

В любом случае, с подобными проблемами сталкиваются не только ГО: они возникают везде, где персональные данные подвергаются «глубокой обработке» в поисках скрытых закономерностей, и особенно обостряются, если к ней добавляются системы машинного обучения, профилирования и автоматического принятия решений. Может показаться, что законодательство о защите данных отстает от всех изменений, однако ОРЗД содержит требования с далеко идущими последствиями для ГО, которые разрабатывают подобные инструменты[116]. В них говорится, что «каждый субъект данных должен иметь право знать и получать сведения в отношении... алгоритма схемы любой автоматизированной обработки персональных данных и последствий такой обработки, если она основана на профилировании», также каждый субъект данных имеет «право требовать людского вмешательства [и] объяснения решения, принятого в результате такой оценки, и для изменения решения»[117].

Более того, «при наличии соответствующей возможности [оператор данных] должен обеспечить удаленный доступ к защищенной системе, которая даст субъекту данных прямой доступ к его/ее персональным данным»[118]. Эти положения легли в основу документа «Руководство по защите лиц в сфере обработки персональных данных в век больших данных (Руководство по большим данным)», опубликованного Советом Европы

116 ОРЗД (примечание 48 выше), преамбула, пп. 63, 71; ст. 4, 13, 14, 15, 22.
117 Там же, преамбула, п. 63.
118 Там же.

в январе 2017 г. Операторов данных призвали не ограничиваться лишь мерами защиты данных, но вводить «профилактические нормы и оценивать риски» в связи с «применением технологий больших данных с правовой, общественной и моральной точки зрения, в том числе и в отношении права на равное обращение и недискриминацию»[119]. Ниже рассмотрено, какими механизмами могут воспользоваться ГО для достижения этих целей.

Биометрические системы

Среди ГО, работающих с мигрантами и беженцами, растет популярность биометрических систем идентификации, поскольку получатели помощи подобных организаций обычно не имеют удостоверений личности. Получив доступ к таким уникальным биометрическим маркерам, как цифровые фотографии, сканы радужной оболочки глаза и отпечатки пальцев, биометрические системы повышают эффективность процесса регистрации, а также ускоряют раздачу гуманитарной помощи, а сам процесс становится более справедливым, потому что сокращается время подтверждения права на помощь и уменьшается число случаев мошенничества. Как уже говорилось, ОРЗД однозначно причисляет биометрические данные к конфиденциальной информации, поэтому защитники конфиденциальности и гражданских свобод постоянно выражают опасения в связи с разработкой и внедрением биометрических систем идентификации. Причина заключается как в масштабе проблем защиты данных и безопасности, возникающих после привязки персональных данных к биометрическому профилю, так и в растущем использовании биометрических систем как инструмента поддержания правопорядка и применения норм законов о мигрантах. Как бы то ни было, явная эффективность и точность биометрического профилирования берут свое. Учитывая, что около 2,4 миллиарда человек не имеют юридических документов, удостоверяющих личность, ООН поставила одной из целей устойчивого развития снабдить их такими удостоверениями, и это стало для государств еще одним стимулом внедрять биометрические системы[120]. Важно также учитывать, что в контексте развития и гуманитарном контексте расширение области использования биометрической регистрации может увеличить масштабы социальной изоляции и даже число людей без гражданства, так как могут быть ущемлены права людей, которым будет отказано в получении гражданства или в праве на защиту, хотя критики систем биометрической идентификации в основном инстинктивно концентрируются на последствиях, возникающих после включения отдельных людей в биометрические базы данных.

Использующие биометрические системы ГО не могут игнорировать подобные опасения. УВКБ, например, уже внедряет в свою работу глобаль-

119 CoE, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*, T-PD (2017) 01, Strasbourg, 23 January 2017 (Big Data Guidelines), p. 5.

120 Цели ООН в области устойчивого развития, «Цель 16: Содействие построению справедливого, миролюбивого и открытого общества», приняты 25 сентября 2015 г., п. 9.

ную Систему управления биометрической информацией (СУБИ), которая еще в течение долгого времени будет служить цифровым средством установления личности людям, исключенным из общественной жизни. УВКБ также использует собранные профили для подтверждения личности и права на получение гуманитарной помощи, чтобы повысить эффективность механизмов распределения продуктов питания и денежной помощи; оно также заслуживает справедливой похвалы за инновационную разработку сложных механизмов обмена данными с оперативными партнерами и банковским сектором Иордании. Но по мере того как все больше государств — членов ООН и партнеров УВКБ начинают внедрять в свою работу биометрические системы либо задумываться об их внедрении или использовании, растет и давление на УВКБ со стороны тех, кто хочет воспользоваться данными или получить доступ к СУБИ для целей, которые не были изначально предусмотрены, например для регистрации беженцев совместно с органами власти страны их пребывания или для проверки отобранных кандидатов на возвращение в страну происхождения с точки зрения угроз безопасности. Как следствие, интересы УВКБ по устранению социальной изоляции вступают в противоречие с государственной политикой насаждения изоляции, что создает в сфере защиты данных и соблюдения основных прав проблемы, которые никто не предвидел в момент, когда формировалась СУБИ. Среди этих проблем — разработка норм, касающихся биометрических данных и систем, которые смогут удовлетворить и противоречивые требования различных заинтересованных сторон, и необходимость объяснять беженцам, как организованы потоки данных и какие присущи этому риски, установят порядок действий в ситуациях, когда получатели помощи и органы власти предъявляют права собственности на данные[121].

Критически важно учитывать, как люди воспринимают эту ситуацию. Любое предположение, что биометрические данные, собранные в гуманитарных целях, могут в итоге быть использованы вопреки интересам получателей помощи, рискует серьезно подорвать доверие ко всем программам, нанести существенный ущерб их репутации и поставить под вопрос само их дальнейшее существование[122]. Даже якобы «низкотехноло-

121 В 2017 г. журнал «Economist» был вынужден задаться вопросом: «Получит ли беженец, лишенный защиты, обусловленной наличием гражданства, право на защиту конфиденциальности персональных данных, хранящихся в облаке?» (“Phones are Now Indispensable for Refugees”, *The Economist*, 11 February 2017, доступно по адресу: https://www.economist.com/international/2017/02/11/phones-are-now-indispensable-for-refugees.

122 В 2016 г. журнал «TakePart» сообщил, что «в январе власти Кале заявили, что в том же месяце они снесут [лагерь беженцев] Джунгли... В качестве альтернативы они объявили об открытии на границе с Джунглями нового официального лагеря беженцев... Но мало кто воспользовался предложением городских властей. Сканеры ладони напугали некоторых жителей лагеря, которые опасались, что их биометрические данные будут переданы полиции и использованы против них, если им удастся добраться до Англии» (Marc Herman, “Unwelcome Refugees”, *TakePart*, 5 February 2016, доступно по адресу: www.takepart.com/feature/2016/02/05/jungle-calais-france-demolition/).

гичные» базы цифровых фотографий неизбежно порождают риски из-за стремительного развития технологий распознавания лиц[123].

Управление рисками

Несмотря на несметное множество рисков, с которыми сталкиваются ГО при обработке персональных данных, и очевидные трудности ответственного внедрения инновационных решений, это никоим образом не означает, что такие проблемы нерешаемы. Любой процесс обработки данных неизбежно порождает риски с точки зрения их защиты, поэтому операторы данных должны в первую очередь правильно оценить их и разработать адекватные меры предосторожности[124]. Такая оценка — не просто способ для ГО «не причинить вреда», она все больше становится юридической обязанностью. Согласно нормам ОРЗД при использовании «новых технологий» оператор перед обработкой должен оценить воздействие планируемых операций обработки на защиту персональных данных, если она «ожидаемо приведет к высокому риску для прав и свобод физических лиц»[125]. Оценка воздействия на защиту персональных данных (ОВЗПД) должна выявить «меры, гарантии и механизмы» минимизации рисков и соответствия нормам закона о защите данных, а результаты необходимо обсудить с субъектами данных[126]. ОВЗПД является обязательной, если оператор намерен задействовать «масштабную обработку» конфиденциальных данных (например, биометрических или медицинских), как и в случае, если автоматизированная обработка носит «систематический и комплексный» характер, включает профилирование и может «существенно [негативно повлиять] на физическое лицо»[127]. Более того, если результаты ОВЗПД «указывают на то, что обработка может привести к возникновению высо-

123 Согласно данным Агентства ЕС по защите основных прав, «во время последнего периода прибытия большого количества беженцев некоторые частные организации стали предлагать услуги розыска, особенно на больших железнодорожных станциях Австрии, Германии и Венгрии, используя фотографии, при этом не учитывались риски, связанные с защитой данных» (EU Fundamental Rights Agency, "Thematic Focus: Family Tracing and Family Reunification", доступно по адресу: fra.europa.eu/en/theme/asylum-migration-borders/overviews/focus-family).

124 Как объясняют Касперсен и Линдсей-Кюрте (примечание 1 выше), «получателям помощи нужно, с одной стороны, давать все самое лучшее, гибко и эффективно помогать нуждающимся, а с другой — это должны делать организации, чья репутация вызывает доверие. Подразумевается, что такие организации готовы в сотрудничестве с партнерами-новаторами совершить переворот, постоянно пересматривать практические подходы к своей работе, серьезно обдумывать возможности технологий по-новому выстраивать связи между людьми, объектами, процессами и данными. Но изыскивая способы воспользоваться огромными возможностями технологий для совершенствования гуманитарной работы, они должны осознавать, что им сопутствуют и очень реальные риски».

125 ОРЗД (примечание 48 выше), ст. 35(1).

126 ОВЗПД должна включать системное описание планируемых операций по обработке данных, а также целей обработки; оценку необходимости и соразмерности операций по обработке с целями обработки; оценку рисков для прав и свобод субъектов данных; меры, запланированные для устранения рисков, включая гарантии, меры безопасности и механизмы обеспечения защиты персональных данных и меры подтверждения соблюдения норм закона о защите данных (см. там же, ст. 35).

127 Там же, ст. 35.

кой степени риска при отсутствии мер, принятых [оператором данных] для снижения риска», то он обязан перед обработкой получить одобрение надзорного органа по защите данных[128]. Недавно опубликованное Советом Европы «Руководство по большим данным» выдвигает операторам данных похожие требования — «определять и оценивать риски каждой операции с данными» и «оценивать потенциальные негативные последствия для соблюдения прав и основных свобод физических лиц»[129]. Также Руководство поощряет оценивать этические последствия, чтобы предотвращать дискриминацию и социальную изоляцию.

По итогам подобной оценки ГО могут снизить риски, присущие конструкции собственных систем ИКТ, разработать на перспективу нормативные документы, в которых будут заложены действенные меры по защите конфиденциальности и основных прав получателей помощи. Стоит надеяться, что этот процесс также преподаст им урок: намного сложнее внедрять механизмы защиты в уже работающие системы, чем предусмотреть их еще на стадии проекта[130]. Именно поэтому последние законы ЕС и Совета Европы требуют, чтобы конструкция подобных систем изначально отвечала нормам конфиденциальности и защиты данных. К счастью, такие требования появились, когда многочисленные инновации, исследования и разработки уже превратили эти когда-то концепции будущего в высокоэффективные средства информационной безопасности и защиты данных. Технологии анонимизации[131], прикладная криптография[132], протоколы «доказательства с нулевым разглашением»[133] и новые возможности, которые дают субъектам данных адекватные и эффективные инструменты контроля[134], уже сегодня позволяют ГО разработать как высокоэффективные, так и высокозащищенные системы ИКТ.

128 ОВЗПД, ст. 36.

129 Big Data Guidelines (примечание 119 выше), p. 5.

130 Однако ОВЗПД может все-таки оказаться полезной, если нужно восполнить пробелы в уже существующих системах и программах.

131 Удалив из массивов данных информацию, по которой можно установить личность человека, либо заменив ее кодами (то есть псевдоминимизировав ее), ГО могут значительно сократить потенциал ее ненадлежащего использования. У этих методов, конечно же, есть свои изъяны (можно «вычислить» личность человека, найдя совпадения данных в нескольких анонимизированных массивах данных, или другими способами создав потенциальную угрозу для тех людей, сведения о которых содержатся в больших совокупных массивах данных), но при правильном применении эти методы могут существенно снизить сопутствующие риски. Однако, как уже отмечалось, анонимизация данных для получения совокупной или статистической информации, которую можно публиковать или как минимум распространять свободнее, чем персональные данные, может в определенных обстоятельствах породить опасные риски с точки зрения защиты получателей помощи (см. примечание 113 выше).

132 Прикладная криптография позволяет шифровать данные — и те, что находятся на хранении, и во время их перемещения.

133 Протоколы «доказательства с нулевым разглашением» используются в хранилищах и не позволяют владельцу хранилища или несанкционированной третьей стороне считывать информацию находящихся там баз данных.

134 Например, персональные системы управления информацией, системы автономных и портативных данных.

Заключение. О каком перевороте идет речь?

После того как четыре года назад организация «Прайваси Интернэшнл» указала на «скудные меры защиты конфиденциальности» в секторах развития и гуманитарной деятельности[135], в гуманитарном секторе достигнут значительный прогресс. Однако многим ГО еще предстоит огромная работа, чтобы достичь минимальных стандартов защиты данных получателей помощи и информационной безопасности, а также ответственно внедрять те инновации, которые соответствуют не только духу, но и букве законов о защите данных. Даже тем организациям, которые стали примером внедрения строгих норм защиты данных, предстоит еще много работы, чтобы в рамках всей своей деятельности добиться должного соблюдения взятых на себя обязательств. Им поможет в этом новый документ МККК «Руководство по защите данных в ходе гуманитарной работы», единственное подробное практическое пособие, которым располагают ГО. При этом жизненно важно продолжать активно развивать обсуждение глобальных стандартов сбора персональных данных, обмена и хранения их в кризисные времена. Те же органы власти, на которые возложены задачи защиты данных, должны взять на себя больше ответственности за разработку и внедрение достижимых стандартов в этой области. Понятно, что ГО, как и все организации, неохотно обсуждают попытки государственных и негосударственных акторов проникнуть в их информационные системы. Однако им придется найти способ совместно решить эту проблему, если они намерены заручиться поддержкой сторонников бескомпромиссного подхода, заложенного в международное гуманитарное право, а также соблюдать нейтралитет и работать эффективно, что и требуется в гуманитарной деятельности. Пока неясно, сможет ли «цифровая Женевская конвенция» решить все эти проблемы, но сейчас ГО крайне важно принять меры для надлежащей защиты своих информационных систем и добиться, чтобы никто не смог использовать их данные и поставить под вопрос их нейтралитет или нанести урон правам и интересам получателей помощи.

Внедрение в гуманитарный сектор инноваций и новых технологий станет ключом в решении этой фундаментальной проблемы. Она в одинаково высокой степени как техническая — требующая ресурсов для оценки серьезных рисков и подлинно ответственного внедрения инноваций вкупе с исследованиями и разработками, — так и ярко выраженная политическая. Ведь до сих пор разговоры о технологическом перевороте в гуманитарной деятельности в очень большой степени характеризуются технологическим детерминизмом, и в подобной риторике необходимость защищать данные зачастую рисуется или воспринимается как помеха. Сегодня эта риторика предполагает, что сотрудники гуманитарных организаций рабо-

135 G. Hosein and C. Nyst (примечание 29 выше).

тают как в «лаборатории», так и «в поле», что они игнорируют новый цифровой гуманитаризм «себе во вред»[136] и это угрожает им «постепенным забвением», если они не совершат «переворот по собственной инициативе»[137]. Еще их предупреждают, что «чрезмерные предписания и строгие нормы, разработанные в совершенно иных обстоятельствах... потенциально могут затормозить открытия», и советуют внедрять «минималистские» подходы к разработке регуляторных механизмов[138].

Конечно, технологии — не более чем способ найти проблему, требующую решения, и понятно, что гуманитарный сектор привлекает множество технологических компаний не просто потому, что они стремятся творить добро, а потому, что для них этот сектор — отличная возможность протестировать в реальном мире собственную продукцию. Если в гуманитарном секторе тон задают ответственные новаторы в стремлении, например, разработать особо защищенные средства связи и хранения данных, то такое сотрудничество будет бесценным. Но когда определяющими становятся иные интересы, возникают серьезные риски появления противоречий в нормах регулирования, нежелательных последствий и развития неблагоприятных внешних факторов. Отчетливо заметно отчаянное стремление некоторых технологических компаний разработать систему управления идентификационными данными беженцев на основе технологии блокчейн[139]. К примеру, они обещают подобным УВКБ учреждениям более надежную и гибкую систему установления личности, но такая система может породить и серьезные риски усугубить или укоренить то отторжение беженцев и ограничение их прав, которым способствует государственная политика, описанная во введении к данной статье. Существенную роль здесь играют и доноры: наконец-то пункты о защите данных стали появляться в соглашениях о пожертвованиях. Но на практике количество взломов и утечек данных может кардинальным образом увеличиться, если чрезмерный приоритет получат программы, основанные на интенсивном использовании данных (например, программы денежных переводов), на биометрических механизмах и механизмах обеспечения прозрачности.

Пока гуманитарный сектор не станет считать технологический переворот и защиту данных взаимно полезными (а не взаимоисключающими) явлениями, ГО неизбежно будут вынуждены принимать плохо обдуманные решения о закупках или разворачивании гуманитарных операций, которые без всякой на то необходимости будут нарушать или подрывать основные права их собственных получателей помощи. Здесь могут

136 См., например, отзывы о книге: Patrick Meier, *Digital Humanitarians: How Big Data is Changing the Face of Humanitarian Response*, Routledge, 2015, доступно по адресу: www.digital-humanitarians.com/.

137 A. Kaspersen and C. Lindsey-Curtet (примечание 1 выше).

138 J. Berens, U. Mans and S. Verhulst (примечание 74 выше), p. 8.

139 "Microsoft and Accenture's Blockchain ID System for Refugees Highlights Data Privacy Needs", *ITU News*, 20 June 2017, доступно по адресу: news.itu.int/blockchain-refugees/.

сыграть самую значимую роль люди, управляющие финансовыми потоками как в самих ГО, так и за их пределами, если они разумным образом выдвинут в качестве приоритета защиту данных и информационной безопасности. В противном случае однажды «катастрофический взлом данных», как его называют специалисты, заставит их прислушаться к вышесказанному.